Log4j Vulnerability - Spotter queries

V 1.0	First Draft	12-12-2021
V 1.1	Updated the conditions for all queries to cover additional patterns of the attack.	21-12-2021

The following queries will help in the identification of the exploit attempts against historical logs. These queries are modeled from the Securonix detection content policies added for log4j CVE-2021-44228. Please make sure to use only the queries compatible with the version of the platform that you are on as between the 6.3 and 6.4 versions, the search syntax and the event schema vary.

Title: Possible CVE-2021-44228 Exploitation Attempt UserAgent Analytic
Description: WEB-SRV9-RUN This query helps in detecting attempts to exploit the Log4J vulnerability having CVE Id CVE-2021-44228 by embedding a malicious payload in the User Agent HTTP header.
Note: UserAgent is typically mapped with requestclientapplication
Applies to version: 6.3.1 and 6.4

Useragent new logic:

```
rg_functionality="Next generation firewall" AND  requestclientapplication CONTAINS "jndi" AND ( requestclientapplication CONTAINS "dns" OR requestclientapplication CONTAINS "ldap" OR requestclientapplication CONTAINS "lower" OR requestclientapplication CONTAINS "rmi" OR requestclientapplication CONTAINS "upper" OR requestclientapplication CONTAINS "nis" OR requestclientapplication CONTAINS "iiop" OR requestclientapplication CONTAINS "corba" OR requestclientapplication CONTAINS "http")

rg_functionality="Next generation firewall" AND ( requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "${env" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "257Bjndi" OR requestclientapplication CONTAINS "$%7Benv" OR requestclientapplication CONTAINS "${base64:" OR requestclientapplication CONTAINS "}${" OR requestclientapplication CONTAINS "${ctx:" OR requestclientapplication CONTAINS "${sd:"
```

OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS ":-j}$")

Index= activity and rg_functionality = "Next generation firewall" and (requestclientapplication contains "%6a" or requestclientapplication contains "%4a" or requestclientapplication contains "%6e" or requestclientapplication contains "%1e" or requestclientapplication contains "%14" or requestclientapplication contains "%64" or requestclientapplication contains "%19" or requestclientapplication contains "%69" or requestclientapplication contains "%3a")

rg_functionality="Web application firewall" AND requestclientapplication CONTAINS "jndi" AND (requestclientapplication CONTAINS "dns" OR requestclientapplication CONTAINS "ldap" OR requestclientapplication CONTAINS "lower" OR requestclientapplication CONTAINS "rmi" OR requestclientapplication CONTAINS "upper" OR requestclientapplication CONTAINS "nis" OR requestclientapplication CONTAINS "iiop" OR requestclientapplication CONTAINS "corba" OR requestclientapplication CONTAINS "http")

rg_functionality="Web application firewall" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "$%7Benv:" OR requestclientapplication CONTAINS "${base64:" OR requestclientapplication CONTAINS "}${" OR requestclientapplication CONTAINS "${ctx:" OR requestclientapplication CONTAINS "${sd:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS ":-j}$")

Index= activity and rg_functionality = "web application firewall" and (requestclientapplication contains "%6a" or requestclientapplication contains "%4a" or requestclientapplication contains "%6e" or requestclientapplication contains "%1e" or requestclientapplication contains "%14" or requestclientapplication contains "%64" or requestclientapplication contains "%19" or requestclientapplication contains "%69" or requestclientapplication contains "%3a")

rg_functionality="web server" AND requestclientapplication CONTAINS "jndi" AND (requestclientapplication CONTAINS "dns" OR requestclientapplication CONTAINS "ldap" OR requestclientapplication CONTAINS "lower" OR requestclientapplication CONTAINS "rmi" OR requestclientapplication CONTAINS "upper" OR requestclientapplication CONTAINS "nis" OR requestclientapplication CONTAINS "iiop" OR requestclientapplication CONTAINS "corba" OR requestclientapplication CONTAINS "http")

rg_functionality="web server" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "$%7Benv:" OR requestclientapplication CONTAINS "${base64:" OR requestclientapplication CONTAINS "}${“ OR requestclientapplication CONTAINS "${ctx:" OR requestclientapplication CONTAINS "${sd:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS ":-j}$")

Index= activity and rg_functionality = "web server" and (requestclientapplication contains "%6a" or requestclientapplication contains "%4a" or requestclientapplication contains "%6e" or requestclientapplication contains "%1e" or requestclientapplication contains "%14" or requestclientapplication contains "%64" or requestclientapplication contains "%19" or requestclientapplication contains "%69" or requestclientapplication contains "%3a")

rg_functionality="Web proxy" AND requestclientapplication CONTAINS "jndi" AND (requestclientapplication CONTAINS "dns" OR requestclientapplication CONTAINS "ldap" OR requestclientapplication CONTAINS "lower" OR requestclientapplication CONTAINS "rmi" OR requestclientapplication CONTAINS "upper"OR requestclientapplication CONTAINS "nis" OR requestclientapplication CONTAINS "iiop" OR requestclientapplication CONTAINS "corba" OR requestclientapplication CONTAINS "http")

rg_functionality="Web proxy" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "$%7Benv:" OR requestclientapplication CONTAINS "${base64:" OR requestclientapplication CONTAINS "}${" OR requestclientapplication CONTAINS "${ctx:" OR requestclientapplication CONTAINS "${sd:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS ":-j}$")

Index= activity and rg_functionality = "Web proxy" and (requestclientapplication contains "%6a" or requestclientapplication contains "%4a" or requestclientapplication contains "%6e" or requestclientapplication contains "%1e" or requestclientapplication contains "%14" or requestclientapplication contains "%64" or requestclientapplication contains "%19" or requestclientapplication contains "%69" or requestclientapplication contains "%3a")

rg_functionality="Authentication / SSO / Single Sign-On" AND requestclientapplication CONTAINS "jndi" AND (requestclientapplication CONTAINS "dns" OR requestclientapplication CONTAINS "ldap" OR requestclientapplication CONTAINS "lower" OR requestclientapplication CONTAINS "rmi" OR requestclientapplication CONTAINS "upper" OR requestclientapplication CONTAINS "nis" OR requestclientapplication CONTAINS "iiop" OR requestclientapplication CONTAINS "corba" OR requestclientapplication CONTAINS "http")

rg_functionality="Authentication / SSO / Single Sign-On" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "${env" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "257Bjndi" OR requestclientapplication CONTAINS "$%7Benv" OR requestclientapplication CONTAINS "${base64:" OR requestclientapplication CONTAINS "}${" OR requestclientapplication CONTAINS "${ctx:" OR requestclientapplication CONTAINS "${sd:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS ":-j}$")

Index= activity and rg_functionality = "Authentication / SSO / Single Sign-On" and (requestclientapplication contains "%6a" or requestclientapplication contains "%4a" or requestclientapplication contains "%6e" or requestclientapplication contains "%1e" or requestclientapplication contains "%14" or requestclientapplication contains "%64" or requestclientapplication contains "%19" or requestclientapplication contains "%69" or requestclientapplication contains "%3a")

rg_functionality="Cloud Authentication / SSO / Single Sign-On" AND requestclientapplication CONTAINS "jndi" AND (requestclientapplication CONTAINS "dns" OR requestclientapplication CONTAINS "ldap" OR requestclientapplication CONTAINS "lower" OR requestclientapplication CONTAINS "rmi" OR requestclientapplication CONTAINS "upper" OR requestclientapplication CONTAINS "nis" OR requestclientapplication CONTAINS "iiop" OR requestclientapplication CONTAINS "corba" OR requestclientapplication CONTAINS "http")

rg_functionality="Cloud Authentication / SSO / Single Sign-On" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "${env"

OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "257Bjndi" OR requestclientapplication CONTAINS "$%7Benv" OR requestclientapplication CONTAINS "${base64:" OR requestclientapplication CONTAINS "}${" OR requestclientapplication CONTAINS "${ctx:" OR requestclientapplication CONTAINS "${sd:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS ":-j}$")

Index= activity and rg_functionality = "Cloud Authentication / SSO / Single Sign-On" and (requestclientapplication contains "%6a" or requestclientapplication contains "%4a" or requestclientapplication contains "%6e" or requestclientapplication contains "%1e" or requestclientapplication contains "%14" or requestclientapplication contains "%64" or requestclientapplication contains "%19" or requestclientapplication contains "%69" or requestclientapplication contains "%3a")

rg_functionality="Authentication / VPN" AND requestclientapplication CONTAINS "jndi" AND (requestclientapplication CONTAINS "dns" OR requestclientapplication CONTAINS "ldap" OR requestclientapplication CONTAINS "lower" OR requestclientapplication CONTAINS "rmi" OR requestclientapplication CONTAINS "upper" OR requestclientapplication CONTAINS "nis" OR requestclientapplication CONTAINS "iiop" OR requestclientapplication CONTAINS "corba" OR requestclientapplication CONTAINS "http")

rg_functionality="Authentication / VPN" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "${env" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "257Bjndi" OR requestclientapplication CONTAINS "$%7Benv" OR requestclientapplication CONTAINS "${base64:" OR requestclientapplication CONTAINS "}${" OR requestclientapplication CONTAINS "${ctx:" OR requestclientapplication CONTAINS "${sd:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS ":-j}$")

Index= activity and rg_functionality = "Authentication / VPN" and (requestclientapplication contains "%6a" or requestclientapplication contains "%4a" or requestclientapplication contains "%6e" or requestclientapplication contains "%1e" or requestclientapplication contains "%14" or requestclientapplication contains "%64" or requestclientapplication contains "%19" or requestclientapplication contains "%69" or requestclientapplication contains "%3a")

rg_functionality="Cloud Services / Applications" AND requestclientapplication CONTAINS "jndi" AND (requestclientapplication CONTAINS "dns" OR requestclientapplication CONTAINS "ldap" OR requestclientapplication CONTAINS "lower" OR requestclientapplication CONTAINS "rmi" OR requestclientapplication CONTAINS "upper" OR requestclientapplication CONTAINS "nis" OR requestclientapplication CONTAINS "iiop" OR requestclientapplication CONTAINS "corba" OR requestclientapplication CONTAINS "http")

rg_functionality="Cloud Services / Applications" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "${env" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "257Bjndi" OR requestclientapplication CONTAINS "$%7Benv" OR requestclientapplication CONTAINS "${base64:" OR requestclientapplication CONTAINS "}${" OR requestclientapplication CONTAINS "${ctx:" OR requestclientapplication CONTAINS "${sd:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS "${map:" OR requestclientapplication CONTAINS ":-j}$")

Index= activity and rg_functionality = "Cloud Services / Applications" and (requestclientapplication contains "%6a" or requestclientapplication contains "%4a" or requestclientapplication contains "%6e" or requestclientapplication contains "%1e" or requestclientapplication contains "%14" or requestclientapplication contains "%64" or requestclientapplication contains "%19" or requestclientapplication contains "%69" or requestclientapplication contains "%3a")

Title: Possible CVE-2021-44228 Exploitation Attempt URI Analytic
Description: WEB-SRV10-RUN This query helps in detecting possible Log4j exploitation patterns in uri on logs
Note: URI/URL is typically mapped with requesturl
Applies to version: 6.3.1, 6.4

rg_functionality="Next generation firewall" AND requesturl CONTAINS "jndi" AND (requesturl CONTAINS "dns" OR requesturl CONTAINS "ldap" OR requesturl CONTAINS "lower" OR requesturl CONTAINS "rmi" OR requesturl CONTAINS "upper" OR requesturl CONTAINS "nis" OR requesturl CONTAINS "iiop" OR requesturl CONTAINS "corba" OR requesturl CONTAINS "http")

rg_functionality="Next generation firewall" AND (requesturl CONTAINS "${upper:" OR requesturl CONTAINS "${lower:" OR requesturl CONTAINS "${::" OR requesturl CONTAINS "%7Bjndi" OR requesturl CONTAINS "$%7Benv" OR requesturl CONTAINS "${base64:" OR requesturl CONTAINS "257Bjndi" OR requesturl CONTAINS "${env:" OR requesturl CONTAINS "}${" OR requesturl CONTAINS "${ctx:" OR requesturl CONTAINS "${sd:" OR requesturl CONTAINS "${map:" OR requesturl CONTAINS "${map:" OR requesturl CONTAINS ":-j}$")

rg_functionality="Web proxy" AND requesturl CONTAINS "jndi" AND (requesturl CONTAINS "dns" OR requesturl CONTAINS "ldap" OR requesturl CONTAINS "lower" OR requesturl CONTAINS "rmi" OR requesturl CONTAINS "upper" OR requesturl CONTAINS "nis" OR requesturl CONTAINS "iiop" OR requesturl CONTAINS "corba" OR requesturl CONTAINS "http")

rg_functionality="Web proxy" AND (requesturl CONTAINS "${upper:" OR requesturl CONTAINS "${lower:" OR requesturl CONTAINS "${::" OR requesturl CONTAINS "$%7Benv" OR requesturl CONTAINS "${base64:" OR requesturl CONTAINS "257Bjndi" OR requesturl CONTAINS "${env:" OR requesturl CONTAINS "%7Bjndi" OR requesturl CONTAINS "}${" OR requesturl CONTAINS "${ctx:" OR requesturl CONTAINS "${sd:" OR requesturl CONTAINS "${map:" OR requesturl CONTAINS "${map:" OR requesturl CONTAINS ":-j}$")

rg_functionality="web server" AND requesturl CONTAINS "jndi" AND (requesturl CONTAINS "dns" OR requesturl CONTAINS "ldap" OR requesturl CONTAINS "lower" OR requesturl CONTAINS "rmi" OR requesturl CONTAINS "upper" OR requesturl CONTAINS "nis" OR requesturl CONTAINS "iiop" OR requesturl CONTAINS "corba" OR requesturl CONTAINS "http"))

rg_functionality="Web server" AND (requesturl CONTAINS "${upper:" OR requesturl CONTAINS "${lower:" OR requesturl CONTAINS "${::" OR requesturl CONTAINS "$%7Benv" OR requesturl CONTAINS "${base64:" OR requesturl CONTAINS "257Bjndi" OR requesturl CONTAINS "${env:" OR requesturl CONTAINS "%7Bjndi" OR requesturl

CONTAINS "}${" OR requesturl CONTAINS "${ctx:" OR requesturl CONTAINS "${sd:" OR requesturl CONTAINS "${map:" OR requesturl CONTAINS "${map:" OR requesturl CONTAINS ":-j}$")

rg_functionality="Web application firewall" AND requesturl CONTAINS "jndi" AND (requesturl CONTAINS "dns" OR requesturl CONTAINS "ldap" OR requesturl CONTAINS "lower" OR requesturl CONTAINS "rmi" OR requesturl CONTAINS "upper" OR requesturl CONTAINS "nis" OR requesturl CONTAINS "iiop" OR requesturl CONTAINS "corba" OR requesturl CONTAINS "http")

rg_functionality="Web application firewall" " AND (requesturl CONTAINS "${upper:" OR requesturl CONTAINS "${lower:" OR requesturl CONTAINS "${:: "OR requesturl CONTAINS "$%7Benv" OR requesturl CONTAINS "${base64:" OR requesturl CONTAINS "257Bjndi" OR requesturl CONTAINS "${env:" OR requesturl CONTAINS "%7Bjndi" OR requesturl CONTAINS "}${" OR requesturl CONTAINS "${ctx:" OR requesturl CONTAINS "${sd:" OR requesturl CONTAINS "${map:" OR requesturl CONTAINS "${map:" OR requesturl CONTAINS ":-j}$")

############## Policy is not created but can be useful for additional searches##############
#RequestContext

rg_functionality="web server" AND requestcontext CONTAINS "jndi" AND (requestcontext CONTAINS "dns" OR requestcontext CONTAINS "ldap" OR requestcontext CONTAINS "lower" OR requestcontext CONTAINS "rmi" OR requestcontext CONTAINS "upper" OR requestcontext CONTAINS "%7Bjndi")

rg_functionality="web server" AND ipaddress NOT NULL AND (requestcontext CONTAINS "${upper:" OR requestcontext CONTAINS "${lower:" OR requestcontext CONTAINS "${::" OR requestcontext CONTAINS "%7Bjndi" OR requestcontext CONTAINS "}${" OR requestcontext CONTAINS "${ctx:" OR requestcontext CONTAINS "${sd:" OR requestcontext CONTAINS "${map:" OR requestcontext CONTAINS "${map:" OR requestcontext CONTAINS ":-j}$")

rg_functionality="Web proxy" AND requestcontext CONTAINS "jndi" AND (requestcontext CONTAINS "dns" OR requestcontext CONTAINS "ldap" OR requestcontext CONTAINS "lower" OR requestcontext CONTAINS "rmi" OR requestcontext CONTAINS "upper" OR requestcontext CONTAINS "%7Bjndi")

```
rg_functionality="Web proxy"  AND ( requestcontext CONTAINS "${upper:" OR
requestcontext CONTAINS "${lower:" OR requestcontext CONTAINS "${::" OR
requestcontext CONTAINS "%7Bjndi" OR requestcontext CONTAINS "}${" OR
requestcontext CONTAINS "${ctx:" OR requestcontext CONTAINS "${sd:" OR
requestcontext CONTAINS "${map:" OR requestcontext CONTAINS "${map:" OR
requestcontext CONTAINS ":-j}$")



rg_functionality="Web application firewall" AND requestcontext CONTAINS "jndi"  AND (
requestcontext CONTAINS "dns" OR requestcontext CONTAINS "ldap" OR requestcontext
CONTAINS "lower" OR requestcontext CONTAINS "rmi" OR requestcontext CONTAINS
"upper" OR requestcontext CONTAINS "%7Bjndi" )



rg_functionality="Web application firewall" AND ( requestcontext CONTAINS "${upper:"
OR requestcontext CONTAINS "${lower:" OR requestcontext CONTAINS "${::" OR
requestcontext CONTAINS "%7Bjndi" OR requestcontext CONTAINS "}${" OR
requestcontext CONTAINS "${ctx:" OR requestcontext CONTAINS "${sd:" OR
requestcontext CONTAINS "${map:" OR requestcontext CONTAINS "${map:" OR
requestcontext CONTAINS ":-j}$")
```

Title: Possible CVE-2021-44228 Exploitation - Unusual Download Attempt From Log4j Logging Server Analytic - Next Generation Firewall

Description: Description: This policy detects download of .class files by an account. If this activity is being observed on a Log4j logging server, then it may indicate successful exploitation of the CVE-2021-44228 Log4j vulnerability on the logging server thereby leading to download of malicious class files that could be loaded into java code.

Note: URI/URL is typically mapped with requesturl; User Agent is mapped with requestclientapplication

Applies to version: 6.3.1 and 6.4

```
rg_functionality = "Next generation firewall" and requestclientapplication contains
"Java" and requesturl ends with ".class" | stats requestclientapplication requesturl
deviceaction
```

Title: Possible CVE-2021-44228 Exploitation - Unusual Download Attempt From Log4j Logging Server Analytic - Web Proxy
Description: Description: PXY-PAN39-RUN This policy detects download of .class files by an account. If this activity is being observed on a Log4j logging server, then it may indicate successful exploitation of the CVE-2021-44228 Log4j vulnerability on the logging server thereby leading to download of malicious class files that could be loaded into java code.
Note: URI/URL is typically mapped with requesturl; User Agent is mapped with requestclientapplication
Applies to version: 6.3.1 and 6.4

```
rg_functionality = "Web Proxy" and requestclientapplication contains "Java" and requesturl ends with ".class" | stats requestclientapplication requesturl eventoutcome
```

Title: Potential Privilege Escalation SamAccountName Spoofing Analytic
Description: Description: WEL-ACC49-RUN This policy detects possible exploitation of the Active Directory Privilege escalation vulnerability CVE-2021-42278 wherein suspicious modification of the Sam Account Name of a machine account is performed. Weaponization of this Windows active directory vulnerability may be observed as a post exploitation scenario after exploitation of the Log4j CVE-2021-44228 vulnerability.
Note: OldTargetUserName is mapped with devicecustomstring3(OldValue in 6.4); NewTargetUserName is mapped with devicecustomsring5(NewValue in 6.4)
Applies to version: 6.3.1 and 6.4

```
index=activity and rg_functionality = "microsoft windows" and baseeventid = 4781 and devicecustomstring3 ends with "$" and devicecustomstring5 not ends with "$"
```

Title: Possible Cryptocurrency Mining CommandLine Analytic - Unix-Linux-AIX
Description: UNX-SYM7-RUN This policy detects cryptocurrency miners by checking for command line strings or arguments associated with common cryptomining tools.

Note: The commandline is mapped to devicecustomstring1.
Applies to version: 6.3.1 and 6.4

```
rg_functionality = "Unix / Linux / AIX" and (devicecustomstring1 contains "xmr" or
devicecustomstring1 contains "cryptonight" or devicecustomstring1 contains "hashrate" or
devicecustomstring1 contains "dockerminer" or devicecustomstring1 contains "oceanhole" or
devicecustomstring1 contains "minergate" or devicecustomstring1 contains "stratum+tcp://" or
devicecustomstring1 contains " --nicehash" OR devicecustomstring1 contains "pool." OR
devicecustomstring1 contains "--coin" OR devicecustomstring1 contains "stratum" OR
devicecustomstring1 contains "elitter.net" OR devicecustomstring1 contains "-a scrypt" OR
devicecustomstring1 "-userpass" OR devicecustomstring1 contains "-max-cpu-usage" OR
devicecustomstring1 contains "qhor.net" OR devicecustomstring1 contains "wallet" OR
devicecustomstring1 contains "--donate-level" OR devicecustomstring1 contains ".xmr1.") |
stats devicecustomstring1
```

Title: Possible CVE-2021-44228 Exploitation Attempt Account Name Analytic
Description: This query helps in detecting attempts to exploit the Log4J vulnerability having CVE Id CVE-2021-44228 by embedding a malicious payload in the accountname.
Applies to version: 6.3.1 and 6.4

```
rg_functionality="Next generation firewall" AND  accountname CONTAINS "jndi" AND (
accountname CONTAINS "dns" OR accountname CONTAINS "ldap" OR accountname
CONTAINS "lower" OR accountname CONTAINS "rmi" OR accountname CONTAINS
"upper" OR accountname CONTAINS "nis" OR accountname CONTAINS "iiop" OR
accountname CONTAINS "corba" OR accountname CONTAINS "http")

rg_functionality="Next generation firewall" AND ( accountname CONTAINS "${upper:" OR
accountname CONTAINS "${lower:" OR accountname CONTAINS "${::" OR accountname
CONTAINS "${env" OR accountname CONTAINS "%7Bjndi" OR accountname CONTAINS
"257Bjndi" OR accountname CONTAINS "$%7Benv" OR accountname CONTAINS
"${base64:" OR accountname CONTAINS "}${" OR accountname CONTAINS "${ctx:" OR
accountname CONTAINS "${sd:" OR accountname CONTAINS "${map:" OR accountname
CONTAINS "${map:" OR accountname CONTAINS ":-j}$" )

Index= activity and rg_functionality = "Next generation firewall" and (accountname contains
"%6a" or accountname contains "%4a" or accountname contains "%6e" or accountname
```

contains "%1e" or accountname contains "%14" or accountname contains "%64" or accountname contains "%19" or accountname contains "%69" or accountname contains "%3a")

rg_functionality="Web application firewall" AND accountname CONTAINS "jndi" AND (accountname CONTAINS "dns" OR accountname CONTAINS "ldap" OR accountname CONTAINS "lower" OR accountname CONTAINS "rmi" OR accountname CONTAINS "upper" OR accountname CONTAINS "nis" OR accountname CONTAINS "iiop" OR accountname CONTAINS "corba" OR accountname CONTAINS "http")

rg_functionality="Web application firewall" AND (accountname CONTAINS "${upper:" OR accountname CONTAINS "${lower:" OR accountname CONTAINS "${::" OR accountname CONTAINS "%7Bjndi" OR accountname CONTAINS "$%7Benv:" OR accountname CONTAINS "${base64:" OR accountname CONTAINS "}${" OR accountname CONTAINS "${ctx:" OR accountname CONTAINS "${sd:" OR accountname CONTAINS "${map:" OR accountname CONTAINS "${map:" OR accountname CONTAINS ":-j}$")

Index= activity and rg_functionality = "web application firewall" and (accountname contains "%6a" or accountname contains "%4a" or accountname contains "%6e" or accountname contains "%1e" or accountname contains "%14" or accountname contains "%64" or accountname contains "%19" or accountname contains "%69" or accountname contains "%3a")

rg_functionality="web server" AND accountname CONTAINS "jndi" AND (accountname CONTAINS "dns" OR accountname CONTAINS "ldap" OR accountname CONTAINS "lower" OR accountname CONTAINS "rmi" OR accountname CONTAINS "upper" OR accountname CONTAINS "nis" OR accountname CONTAINS "iiop" OR accountname CONTAINS "corba" OR accountname CONTAINS "http")

rg_functionality="web server"   AND (accountname CONTAINS "${upper:" OR accountname CONTAINS "${lower:" OR accountname CONTAINS "${::" OR accountname CONTAINS "%7Bjndi" OR accountname CONTAINS "$%7Benv:" OR accountname CONTAINS "${base64:" OR accountname CONTAINS "}${“ OR accountname CONTAINS "${ctx:" OR accountname CONTAINS "${sd:" OR accountname CONTAINS "${map:" OR accountname CONTAINS "${map:" OR accountname CONTAINS ":-j}$")

Index= activity and rg_functionality = "web server" and (accountname contains "%6a" or accountname contains "%4a" or accountname contains "%6e" or accountname contains "%1e" or accountname contains "%14" or accountname contains "%64" or accountname contains "%19" or accountname contains "%69" or accountname contains "%3a")

rg_functionality="Web proxy" AND accountname CONTAINS "jndi" AND (accountname CONTAINS "dns" OR accountname CONTAINS "ldap" OR accountname CONTAINS "lower" OR accountname CONTAINS "rmi" OR accountname CONTAINS "upper"OR

accountname CONTAINS "nis" OR accountname CONTAINS "iiop" OR accountname CONTAINS "corba" OR accountname CONTAINS "http")
rg_functionality="Web proxy" AND (accountname CONTAINS "${upper:" OR accountname CONTAINS "${lower:" OR accountname CONTAINS "${::" OR accountname CONTAINS "%7Bjndi" OR accountname CONTAINS "$%7Benv:" OR accountname CONTAINS "${base64:" OR accountname CONTAINS "}${" OR accountname CONTAINS "${ctx:" OR accountname CONTAINS "${sd:" OR accountname CONTAINS "${map:" OR accountname CONTAINS "${map:" OR accountname CONTAINS ":-j}$")

Index= activity and rg_functionality = "Web proxy" and (accountname contains "%6a" or accountname contains "%4a" or accountname contains "%6e" or accountname contains "%1e" or accountname contains "%14" or accountname contains "%64" or accountname contains "%19" or accountname contains "%69" or accountname contains "%3a")

rg_functionality="Authentication / VPN" AND accountname CONTAINS "jndi" AND (accountname CONTAINS "dns" OR accountname CONTAINS "ldap" OR accountname CONTAINS "lower" OR accountname CONTAINS "rmi" OR accountname CONTAINS "upper" OR accountname CONTAINS "nis" OR accountname CONTAINS "iiop" OR accountname CONTAINS "corba" OR accountname CONTAINS "http")

rg_functionality="Authentication / VPN" AND (accountname CONTAINS "${upper:" OR accountname CONTAINS "${lower:" OR accountname CONTAINS "${::" OR accountname CONTAINS "${env" OR accountname CONTAINS "%7Bjndi" OR accountname CONTAINS "257Bjndi" OR accountname CONTAINS "$%7Benv" OR accountname CONTAINS "${base64:" OR accountname CONTAINS "}${" OR accountname CONTAINS "${ctx:" OR accountname CONTAINS "${sd:" OR accountname CONTAINS "${map:" OR accountname CONTAINS "${map:" OR accountname CONTAINS ":-j}$")

Index= activity and rg_functionality = "Authentication / VPN" and (accountname contains "%6a" or accountname contains "%4a" or accountname contains "%6e" or accountname contains "%1e" or accountname contains "%14" or accountname contains "%64" or accountname contains "%19" or accountname contains "%69" or accountname contains "%3a")

rg_functionality="Authentication / SSO / Single Sign-On" AND accountname CONTAINS "jndi" AND (accountname CONTAINS "dns" OR accountname CONTAINS "ldap" OR accountname CONTAINS "lower" OR accountname CONTAINS "rmi" OR accountname CONTAINS "upper" OR accountname CONTAINS "nis" OR accountname CONTAINS "iiop" OR accountname CONTAINS "corba" OR accountname CONTAINS "http")

rg_functionality="Authentication / SSO / Single Sign-On" AND (accountname CONTAINS "${upper:" OR accountname CONTAINS "${lower:" OR accountname CONTAINS "${::" OR

accountname CONTAINS "${env" OR accountname CONTAINS "%7Bjndi" OR accountname CONTAINS "257Bjndi" OR accountname CONTAINS "$%7Benv" OR accountname CONTAINS "${base64:" OR accountname CONTAINS "}${" OR accountname CONTAINS "${ctx:" OR accountname CONTAINS "${sd:" OR accountname CONTAINS "${map:" OR accountname CONTAINS "${map:" OR accountname CONTAINS ":-j}$")

Index= activity and rg_functionality = "Authentication / SSO / Single Sign-On" and (accountname contains "%6a" or accountname contains "%4a" or accountname contains "%6e" or accountname contains "%1e" or accountname contains "%14" or accountname contains "%64" or accountname contains "%19" or accountname contains "%69" or accountname contains "%3a")

rg_functionality="Cloud Authentication / SSO / Single Sign-On" AND accountname CONTAINS "jndi" AND (accountname CONTAINS "dns" OR accountname CONTAINS "ldap" OR accountname CONTAINS "lower" OR accountname CONTAINS "rmi" OR accountname CONTAINS "upper" OR accountname CONTAINS "nis" OR accountname CONTAINS "iiop" OR accountname CONTAINS "corba" OR accountname CONTAINS "http")

rg_functionality="Cloud Authentication / SSO / Single Sign-On" AND (accountname CONTAINS "${upper:" OR accountname CONTAINS "${lower:" OR accountname CONTAINS "${::" OR accountname CONTAINS "${env" OR accountname CONTAINS "%7Bjndi" OR accountname CONTAINS "257Bjndi" OR accountname CONTAINS "$%7Benv" OR accountname CONTAINS "${base64:" OR accountname CONTAINS "}${" OR accountname CONTAINS "${ctx:" OR accountname CONTAINS "${sd:" OR accountname CONTAINS "${map:" OR accountname CONTAINS "${map:" OR accountname CONTAINS ":-j}$")

Index= activity and rg_functionality = "Cloud Authentication / SSO / Single Sign-On" and (accountname contains "%6a" or accountname contains "%4a" or accountname contains "%6e" or accountname contains "%1e" or accountname contains "%14" or accountname contains "%64" or accountname contains "%19" or accountname contains "%69" or accountname contains "%3a")

rg_functionality="Cloud Services / Applications" AND accountname CONTAINS "jndi" AND (accountname CONTAINS "dns" OR accountname CONTAINS "ldap" OR accountname CONTAINS "lower" OR accountname CONTAINS "rmi" OR accountname CONTAINS "upper" OR accountname CONTAINS "nis" OR accountname CONTAINS "iiop" OR accountname CONTAINS "corba" OR accountname CONTAINS "http")

rg_functionality="Cloud Services / Applications" AND (accountname CONTAINS "${upper:" OR accountname CONTAINS "${lower:" OR accountname CONTAINS "${::" OR accountname CONTAINS "${env" OR accountname CONTAINS "%7Bjndi" OR

accountname CONTAINS "257Bjndi" OR accountname CONTAINS "$%7Benv" OR accountname CONTAINS "${base64:" OR accountname CONTAINS "}${" OR accountname CONTAINS "${ctx:" OR accountname CONTAINS "${sd:" OR accountname CONTAINS "${map:" OR accountname CONTAINS "${map:" OR accountname CONTAINS ":-j}$")

Index= activity and rg_functionality = "Cloud Services / Applications" and (accountname contains "%6a" or accountname contains "%4a" or accountname contains "%6e" or accountname contains "%1e" or accountname contains "%14" or accountname contains "%64" or accountname contains "%19" or accountname contains "%69" or accountname contains "%3a")

Title: Possible CVE-2021-44228 Exploitation -Log4j related signature detection - IDS-IPS
Description: This policy will trigger whenever the string related to Log4j vulnerability matches in the signature name of the IPS/IDS product.
Note: The Signature is mapped to message.
Applies to version: 6.3.1 and 6.4

rg_functionality = "IDS / IPS / UTM / Threat Detection" and (message CONTAINS "log4j" OR message CONTAINS "CVE-2021-44228" OR message CONTAINS "JNDI" OR message CONTAINS "CVE_2021_44228" OR message CONTAINS "Log4Shell" OR message CONTAINS "2021-44228")

Title: Possible CVE-2021-44228 Exploitation -Log4j related signature detection - Cloud EDR
Description: This policy will trigger whenever the string related to Log4j vulnerability matches in the signature name of the AV/Malware/EDR product.
Note: The Signature is mapped to message.
Applies to version: 6.3.1 and 6.4

rg_functionality = "Cloud Antivirus / Malware / EDR" and (message CONTAINS "log4j" OR message CONTAINS "CVE-2021-44228" OR message CONTAINS "JNDI" OR message CONTAINS "CVE_2021_44228" OR message CONTAINS "Log4Shell" OR message CONTAINS "2021-44228")

Title: Possible CVE-2021-44228 Exploitation -Log4j related signature detection - EDR

Description: This policy will trigger whenever the string related to Log4j vulnerability matches in the signature name of the AV/Malware/EDR product.

Note: The Signature is mapped to message.

Applies to version: 6.3.1 and 6.4

```
rg_functionality = "Antivirus / Malware / EDR" and  ( message CONTAINS "log4j" OR message CONTAINS "CVE-2021-44228" OR message CONTAINS "JNDI" OR message CONTAINS "CVE_2021_44228" OR message CONTAINS "Log4Shell" OR message CONTAINS "2021-44228" )
```

Title: Possible CVE-2021-44228 Exploitation -Log4j related signature detection - Web Application Firewall

Description: This policy will trigger whenever the string related to Log4j vulnerability matches in the signature name of the WAF product.

Note: The Signature is mapped to message.

Applies to version: 6.3.1 and 6.4

```
rg_functionality = "Web Application Firewall" and  ( message CONTAINS "log4j" OR message CONTAINS "CVE-2021-44228" OR message CONTAINS "JNDI" OR message CONTAINS "CVE_2021_44228" OR message CONTAINS "Log4Shell" OR message CONTAINS "2021-44228" )
```