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 "%7Bjndi")

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 "}${" OR requestclientapplication CONTAINS "${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" OR requestclientapplication CONTAINS "%7Bjndi")

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 "%7Bjndi")

rg_functionality="Web application firewall" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "}${" 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" OR requestclientapplication CONTAINS "%7Bjndi")

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 "%7Bjndi")

rg_functionality="web server" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "}${“ 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" OR requestclientapplication CONTAINS "%7Bjndi")

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 "%7Bjndi")

rg_functionality="Web proxy" AND (requestclientapplication CONTAINS "${upper:" OR requestclientapplication CONTAINS "${lower:" OR requestclientapplication CONTAINS "${::" OR requestclientapplication CONTAINS "%7Bjndi" OR requestclientapplication CONTAINS "}${" 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" OR requestclientapplication CONTAINS "%7Bjndi")

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")

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

rg_functionality="Web 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")

rg_functionality="Web proxy" AND (requesturl CONTAINS "${upper:" OR requesturl CONTAINS "${lower:" OR requesturl CONTAINS "${::" OR requesturl CONTAINS "%7Bjndi" OR requesturl CONTAINS "}${" 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 "%7Bjndi"))

rg_functionality="Web server" AND (requesturl CONTAINS "${upper:" OR requesturl CONTAINS "${lower:" OR requesturl CONTAINS "${::" OR requesturl CONTAINS "%7Bjndi" OR requesturl CONTAINS "}${" 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")

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

#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.
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") | stats devicecustomstring1
```

Title: Possible CVE-2021-44228 Exploitation - Potential Malicious Commands Execution From Log4j Logging Server Parent-Child Analytic - Microsoft Windows
Description: Detect potential malicious commands from java application.
Applies to version: 6.3.1 and 6.4

```
rg_functionality = "Microsoft Windows" and sourceprocessname ends with java.exe and (filepath contains sh or filepath contains bash or filepath contains dash or filepath contains ksh or filepath contains tcsh or filepath contains zsh or filepath contains curl or filepath contains perl or filepath contains python or filepath contains ruby or filepath contains php or filepath contains wget) | stats filepath
```

Title: Possible CVE-2021-44228 Exploitation - Potential Malicious Commands Execution From Log4j Logging Server Parent-Child Analytic - Unix-Linux-AIX
Description: UNX-SYM9-RUN - Detect potential malicious commands from java application.
Applies to version: 6.3.1 and 6.4

```
rg_functionality = "Unix / Linux / AIX" and sourceprocessname ends with java.exe and (filepath contains sh or filepath contains bash or filepath contains dash or filepath contains ksh or filepath contains tcsh or filepath contains zsh or filepath contains curl or filepath contains perl or filepath contains python or filepath contains ruby or filepath contains php or filepath contains wget) | stats filepath
```

Title: Possible CVE-2021-44228 Exploitation - Unusual LDAPs Network Connection From Java Application - EMS
Description: Detect LDAP/LDAPS connections to external destinations
Applies to version: 6.3.1 and 6.4

```
rg_functionality="Endpoint Management Systems" and deviceeventcategory / deviceaction IN (netconn,DnsRequest,NetworkConnectIP4,NetworkReceiveAcceptIP4,NetworkListenIP6,Network connection detected,NetworkCloseIP4,SuspiciousDnsRequest,NetworkConnectIP6,NetworkReceiveAcceptIP6,Trace Network Connections,NetworkListenIP4) and (sourceprocessname contains "tomcat.exe" or destinationprocessname contains "tomcat.exe" or filename contains "tomcat.exe" or sourceprocessname contains "java.exe" or destinationprocessname contains "java.exe" or filename contains "java.exe" ) and ( destinationport=389 OR destinationport=636 OR destinationport=1389 OR destinationport=10389 OR destinationport=10636 OR destinationport=1099 OR destinationport=53 OR destinationport=5353 ) AND destinationaddress NOT IN (10.0.0.0/8,172.16.0.0/16,192.168.0.0/16)
```

Title: Possible CVE-2021-44228 Exploitation - Unusual LDAPs Network Connection From Java Application - Unix-Linux-AIX
Description: Description: UNX-SYM8-RUN - Detect LDAP/LDAPS connections to external destinations.
Applies to version: 6.3.1 and 6.4

```
rg_functionality = "Unix / Linux / AIX" and (filepath ends with java.exe or sourceprocessname ends with java.exe) and (destinationport = 389 or destinationport = 636 or destinationport = 1389 or destinationport = 10389 or destinationport = 10636 or destinationport = 1099 or destinationport = 53 or destinationport = 5353) AND destinationaddress NOT IN (10.0.0.0/8,172.16.0.0/16,192.168.0.0/16) | stats destinationaddress deviceaction
```