Indusface Security Bulletin

Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)

December 2021

What is Apache Log4j Remote Code Execution (CVE-2021-44228) Vulnerability?

Log4j 2 is a logging library used in many Java applications and services. The library is part of the Apache Software Foundation's Apache Logging Services project. A remote code execution vulnerability exists in Apache Log4j2 <=2.14.1 JNDI features where configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI-related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when the message lookup substitution is enabled. This vulnerability is also known as "Log4Shell".

What Are the Risks?

A remote attacker can exploit the vulnerability without authentication and successful exploitation can grant full control of the victim's system. This is known to be actively being exploited in wild as the POCs are available in public.

Severity: Critical

CVSSv3.1: Base Score: 10.0 CRITICAL
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSSv2: Base Score: 9.3 HIGH

Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C)

Exploit available in public: Yes

Exploit complexity: Low

Do You Need to Worry About It?

The vendor has released the security patch and we strongly advise our customers to update their installations as soon as possible.

Mitigation

1) Upgrade it to Log4j v2.15.0, vulnerability is patched from this version.

2) If you are using a vulnerable version and cannot upgrade, then set the below parameter:

log4j2.formatMsgNoLookups=true

Additionally, an environment variable can be set for these all the affected versions:

LOG4J_FORMAT_MSG_NO_LOOKUPS=true

3) Alternatively, the JndiLookup class can be removed with the help of similar command as below:

zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
to remove the class from the log4j-core.

Product Coverage:

Indusface AppTrana blocks exploits targeting the Log4J vulnerability (CVE-2021-44228) and customers behind AppTrana WAF are protected. We highly recommend customers to still take the above mentioned mitigation steps. Protection against this vulnerability was rolled out on Dec 11th.

We are working on enabling coverage for this vulnerability in Indusface WAS. At this point we recommend to our customers to check if they are using Log4j in their environment and if so then upgrade to latest version and follow mitigation steps mentioned above.