TLP: White[1]

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

(Supplement)

Dear Constituents,

This is a supplement to our previous advisory that we issued on 13th December 2021, regarding the Log4J vulnerability (**CVE-2021-44228**). It has come to our attention that this vulnerability has affected various software products including online services and web applications.

According to security researchers and the security community, a massive exploitation campaign is currently ongoing with different threat actors including Nation State backed groups from different countries looking to exploit the vulnerability. It has been reported that the threat actors are exploiting the vulnerability to install various malware, including coin miners and botnets. There has also been instances reported that different ransomware families are being installed by exploiting this vulnerability.

Please be aware that another vulnerability has been found in Log4J 2.15.0 (**CVE-2021-45046**) which we recommended in our previous advisory to update to. An updated version has been released to patch this vulnerability.

What to do

Be sure to follow the steps below:

1. We urge constituents to urgently patch Log4J to the latest version (2.16.0 is now available).
2. Find out if any of the products or applications deployed in your network use the Log4J library and please follow the respective vendor's advisory on how to address this vulnerability.
    a. Please refer here to a list of software and its vulnerability status as provided by National Cyber Security Center- Netherland (NCSC-NL). On

1 CERT Tonga adopts the Traffic Light Protocol

this page NCSC-NL will maintain a list of all known vulnerable and not vulnerable software. Furthermore, any reference to the software will contain specific information regarding which version contains the security fixes, and software still requires mitigation.

3. There is a possibility your systems might have been compromised prior to patching. As such, we highly recommend that you update your detection signatures and carry out a full system scan as well as stepping up your detection and monitoring for abnormal behavior.
4. Ensure that you apply the following steps before going on Christmas break to make sure that there is no disruption during the holidays.

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