SERVICE FACTS on SECURITY NOTICE
APACHE LOG4J VULNERABILITY
(PSS-IS-2021-121000)

Within the past days, the Fujitsu PSIRT received open-source intelligence on a new threat referred to as Log4Shell.

Log4Shell is a an RCE (Remote Code Execution) 0-day exploit, found in the log4j logging software. That exploit allows to mount successful and effective attacks against victims running named Java logging library. According to the researchers, the impact of the exploit is to gain full system control.

The Fujitsu PSIRT has knowledge of working PoC (Proof of Concept) code, able to potentially employ Log4Shell, not requiring any elevated or otherwise special permissions on a given victim system, except for remote connectivity.

The U.S. NIST ITL and other bodies have already reported on Log4Shell (CVE-2021-44228), while assigning a CVSSv3.1 base score of Critical (10.0).

The Fujitsu PSIRT has not yet estimated a Fujitsu ARF (Affection Risk Factor), based on log4j prevalence, log4j security record, and log4j fix/mitigation expenditure. However, the currently estimated Fujitsu ARF is Medium (3).

The Fujitsu PSIRT would like to inform its customer base, that the present Apache log4j vulnerability was addressed internally already.
SOLUTION / REMEDIATION

Based on the intelligence information available, the Fujitsu PSIRT rated the Log4Shell exploit and its underlying log4j vulnerability as a medium-level threat to Fujitsu products, in part due to the limited overall prevalence of vulnerable log4j packages in Fujitsu products.

Due to the nature of the Log4Shell exploit, the Fujitsu PSIRT already notified all Fujitsu PSIRT members, as well as adjacent development and engineering departments.

The Fujitsu PSIRT requested a fix of the underlying vulnerability, via software package updates, and has also provided further instructions on immediate log4j vulnerability mitigation. Fujitsu product updates will be made available consecutively, as soon as all intelligence provided by the Fujitsu PSIRT was processed.

ADDITIONAL INFORMATION

At this point Fujitsu PSIRT issue PSS-IS-2021-121000, addressing the Log4Shell exploit and corresponding log4j vulnerability, is IN PROGRESS and will be updated in regular intervals, within the Fujitsu PSIRT PRODUCT SECURITY section of the Fujitsu (EMEA) Product Support website.

A brief ACL (List of Affected Fujitsu Categories & Products) will be added to this document, as soon as all product-related information was received and processed by the Fujitsu PSIRT.

There are no further recommendations by the Fujitsu PSIRT on the mitigation of this vulnerability.