SKF Response to CVE-2021-44228 Apache Log4j

Customer information

SKF is aware of a major security vulnerability that has been identified within the widely used open-source platform Log4J. SKF have started all actions needed in relation to mitigating action and progressing well.

Summary

SKF continues our analysis of the remote code execution vulnerability (CVE-2021-44228) related to Apache Log4j (a logging tool used in many Java-based applications) disclosed on 9 Dec 2021.

In addition to monitoring the threat landscape for attacks and developing customer protections, our security teams have been analyzing our products and services to understand where Apache Log4j may be used and are taking expedited steps to mitigate any instances. If we identify any impact to customer data, we will notify the affected party.

Analysis of the CVE-2021-44228 vulnerability

The vulnerability is a remote code execution vulnerability that can allow an unauthenticated attacker to gain complete access to a target system. It can be triggered when a specially crafted string is parsed and processed by the vulnerable Log4j 2 component. This could happen through any user provided input.

Successful exploitation allows for arbitrary code execution in the targeted application. Attackers do not need prior access to the system to log the string and can remotely cause the logging event by using commands like curl against a target system to log the malicious string in the application log. When processing the log, the vulnerable system reads the string and executes it, which in current attacks is used to execute the code from the malicious domain. Doing so can grant the attacker full access and control of the affected application.