



# PRODUCT SECURITY ADVISORY

December 20, 2021

---

| PSIRT Record Number               |
|-----------------------------------|
| <a href="#">CARR-PSA-003-1221</a> |

## Overview

On December 10, 2021, [CVE-2021-44228](#) was published as a Remote Code Execution vulnerability in the Apache Log4j library, a Java-based logging utility. This vulnerability allows an attacker who can control log messages to execute arbitrary code loaded from attacker-controlled servers. Apache quickly released Log4j 2.15.0 to resolve the vulnerability.

December 13, 2021, [CVE-2021-4104](#) Increases the scope to include Log4j 1.2.x

December 14, 2021, [CVE-2021-45046](#) It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. Apache responded with the release of Log4j 2.16.

December 18, 2021, [CVE-2021-45105](#) It was found that the fix to address CVE-2021-45046 in Apache Log4j 2.16 did not protect from uncontrolled recursion from self-referential lookups. This results in a StackOverflow error that will terminate the process, also known as a DOS (Denial of Service) attack. Apache responded with the release of Log4j 2.17.



## PSIRT Statement

Carrier is rapidly working to determine if any of our offerings may be impacted by the Log4j vulnerability. Should we determine that any of our offerings were impacted, additional information regarding mitigations or other actions in response to this matter will follow as our investigation unfolds. More information about vulnerabilities is provided by the Apache Foundation at [Log4j – Apache Log4j Security Vulnerabilities](#).

## About Carrier Product Security Incident Response Team (PSIRT)

PSIRT focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within Carrier products, offerings, solutions, components and/or services. PSIRT is a dedicated team of first responders responsible to deliver advanced support designed to contain and minimize the spread and impact of a product security event, incident, breach, and/or crises.

For more information about Global Product Security and PSIRT, please visit us as: <https://www.corporate.carrier.com/product-security/>

To inquire about this, or any, security issue related to a Carrier offering, contact us at: [productsecurity@carrier.com](mailto:productsecurity@carrier.com)

| Initial Publication Date | Last Published Date |
|--------------------------|---------------------|
| December 20, 2021        | December 20, 2021   |