



Advisory Alert

Alert Number: AAA20211229

Date: December 29, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Apache	Medium	Remote Code Execution

Description

Affected Product	Apache
Severity	Medium
Affected Vulnerability	Remote Code Execution (CVE-2021-44832)
Description	Apache Log4j2 versions 2.0-beta7 through 2.17.0 contain a vulnerability that could allow an attacker with permission to modify the logging configuration file to execute arbitrary code, when the JDBC Appender is used. Apache highly recommends to apply necessary security fixes to avoid issues.
Affected Products	All versions from 2.0-alpha7 to 2.17.0, excluding 2.3.2 and 2.12.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://logging.apache.org/log4j/2.x/security.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka

Hotline: + 94 112039777