Advisory Alert

Alert Number: AAA20220218 **Date:** February 18, 2022

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities

Description

Affected Product	IBM
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23307, CVE-2022-23305, CVE-2022-23302)
Description	IBM has released Security Updates addressing for multiple vulnerabilities. IBM WebSphere Application Server and IBM WebSphere Application Server Liberty are vulnerable to arbitrary code execution and SQL injection due to Apache Log4j. CVE-2022-23307 - Apache Log4j could allow a remote attacker to execute arbitrary code on the system, caused by an unsafe deserialization in the in Apache Chainsaw component. By sending specially crafted input, an attacker could exploit this vulnerability to execute arbitrary code on the system. CVE-2022-23305 - A remote attacker could send specially crafted SQL statements to the JDBCAppender, which could allow the attacker to view, add, modify or delete information in the back-end database. CVE-2022-23302 - Apache Log4j could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unsafe deserialization in JMSSink. By sending specially-crafted JNDI requests using TopicConnectionFactoryBindingName configuration, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM highly recommends applying relevant patches at the earliest to avoid issues.
Affected Products	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 IBM WebSphere Application Server Liberty 17.0.0.3 - 21.0.0.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6557248

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.