Advisory Alert

Alert Number: AAA20221227 **Date:** December 27, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-2163, CVE-2022-21541, CVE-2022-21540)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in the IBM SDK Java Technology Edition that is shipped with IBM WebSphere Application Server. **CVE-2021-2163 –** An unspecified vulnerability exists in Java SE related to the Libraries component that is used in the IBM WebSphere application server. Using this vulnerability an unauthenticated attacker can cause no confidentiality impact, high integrity impact, and no availability impact. **CVE-2022-21541 -** An unspecified vulnerability exists in Java SE related to the VM component that is used in the IBM WebSphere application Server. Using this vulnerability an unauthenticated attacker can cause no confidentiality impact, high integrity impact, and no availability impact. **CVE-2022-21540 -** An unspecified vulnerability exists in Java SE related to the VM component that is used in the IBM WebSphere application Server. Using this vulnerability an unauthenticated attacker can obtain sensitive information resulting in a low confidentiality impact using unknown attack vectors. IBM recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	IBM Java SDK shipped with IBM WebSphere Application Server Patterns 1.0.0.0 through 1.0.0.7 and 2.2.0.0 through 2.3.3.5.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6851613

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.