# Advisory Alert

**Alert Number:** AAA20210216 **Date:** February 16, 2021

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **IBM WebSphere** | **High** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **IBM WebSphere** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2020-2773, CVE-2020-14782, CVE-2020-27221, CVE-2020-14781) |
| Description | IBM has released security patch updates addressing Multiple Vulnerabilities in the WebSphere Application Server product.<br>**CVE-2020-2773** - That are affected Supported versions of Java SE: 7u251, 8u241, 11.0.6 and 14. Vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE and Java SE Embedded. This vulnerability can result in unauthorized ability to cause a partial denial of service in Java SE, Java SE Embedded<br>**CVE-2020-14782** - This vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE and Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data.<br>**CVE-2020-27221** - There is potential for a stack-based buffer overflow when the virtual machine or JNI natives are converting from UTF-8 characters to platform encoding.<br>**CVE-2020-14781** - This vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE and Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE and Java SE Embedded accessible data |
| Affected Products | WebSphere Application Server Continuous Delivery<br>WebSphere Application Server 9.0<br>WebSphere Application Server 8.5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/6415639 |

## 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.**