Advisory Alert

Alert Number : AAA20210322 **Date :** March 22, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**, **Medium**	**Multiple Vulnerabilities**

Description

Affected Product	**IBM**
Severity	**High -** CVE-2020-5025, **Medium** CVE-2020-4976 , CVE-2020-5016
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-4976 CVE-2020-5025 CVE-2020-5016)
Description	IBM released security patch updates addressing Multiple vulnerabilities **CVE-2020-4976** - IBM DB2 for Linux, UNIX and Windows B2 Connect Server could allow a local user to read and write specific files due to weak file permissions **CVE-2020-5025** - IBM DB2 for Linux, UNIX and Windows DB2 Connect Server db2fm is vulnerable to a buffer overflow, caused by improper bounds checking which could allow a local attacker to execute arbitrary code on the system with root privileges. **CVE-2020-5016** - IBM WebSphere Application Server could allow a remote attacker to traverse directories on the system. When application security is disabled and JAX-RPC applications are present, an attacker could send a specially-crafted URL request containing "dot dot" sequences to view arbitrary xml files on the system. This does not occur if Application security is enabled
Affected Products	IBM Db2 V9.7, V10.1, V10.5, V11.1, and V11.5 IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 - Tivoli System
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	**IBM Db2** https://www.ibm.com/support/pages/node/6427859 https://www.ibm.com/support/pages/node/6427855 **IBM Web Sphere Application Server** https://www.ibm.com/support/pages/node/6434125

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.