Advisory Alert

Alert Number: AAA20201216 **Date:** December 16, 2020

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Multiple Vulnerabilities

Description

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security patch updates addressing multiple vulnerabilities that exist in their products. IBM highly recommends to apply relevant patches at earliest to avoid issues. **CVE-2019-12400** - Apache Santuario XML Security for Java could allow a remote attacker to bypass security restrictions, caused by the loading of XML parsing code from an untrusted source. **CVE-2014-3607 -** Ldaptive could allow a remote attacker to conduct a spoofing attack in DefaultHostnameVerifier, caused by the failure to properly verify that the server hostname matches a domain name in the subject's Common Name (CN) field of the X.509 certificate. **CVE-2020-13692 -** PostgreSQL JDBC Driver could allow a remote authenticated attacker to obtain sensitive information, caused by an XML external entity (XXE) error when processing XML data. By sending specially crafted XML data, a remote attacker could exploit this vulnerability to obtain sensitive information. **CVE-2020-2601 -** An unspecified vulnerability in Oracle Java SE related to the Java SE, Java SE Embedded Security component could allow an unauthenticated attacker to obtain sensitive information resulting in a high confidentiality impact using unknown attack vectors.
Affected Products	IBM QRadar 7.3.0 to 7.3.3 Patch 5 IBM QRadar 7.4.0 to 7.4.1 Patch 1 WebSphere Cast Iron v 7.5.0.0, 7.5.0.1, 7.5.1.0 WebSphere Cast Iron v 7.0.0.0, 7.0.0.1, 7.0.0.2 App Connect Professional v 7.5.2.0 App Connect Professional v 7.5.3.0 App Connect Professional v 7.5.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6382284 https://www.ibm.com/support/pages/node/6382288 https://www.ibm.com/support/pages/node/6382286 https://www.ibm.com/support/pages/node/6382172

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.