TLP: WHITE

Advisory Alert

Alert Number: **AAA20220930** **Date:** **September 30, 2022**

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 (CVE-2022-2191, CVE-2022-2047, CVE-2022-2048, CVE-2022-24823, CVE-2020-36518, CVE-2022-24785)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in the moment.js and Zookeeper that used in the IBM QRadar User Behavior Analytics product. **CVE-2022-2191** - A Denial of Service vulnerability exists in the Eclipse Jetty that is used in the Zookeeper because of a flaw with SslConnection which does not release ByteBuffers from the configured ByteBufferPool in the case of error code paths. A remote attacker could exploit this by sending a specially-crafted request. **CVE-2022-2047** - A security restriction bypass vulnerability exists in Eclipse Jetty that is used in the Zookeeper, due to a flaw in the HttpURI class. An attacker could exploit this vulnerability by sending a specially-crafted request. **CVE-2022-2048** - A Denial of Service vulnerability exists in the Eclipse Jetty that is used in the Zookeeper, due to a flaw in the error handling of an invalid HTTP/2 request. A remote attacker could exploit this vulnerability to cause the server to become unresponsive, resulting in a denial of service condition. **CVE-2022-24823** - Sensitive information disclosure vulnerabilities exist in Netty that is used in the Zookeeper, due to a flaw that is caused when temporary upload storage on disc is enabled. An attacker could exploit this vulnerability by gaining access to the local system temporary directory. **CVE-2020-36518** - A Denial of Service vulnerability exists in the FasterXML jackson-databind that is used in the Zookeeper. The flaw is caused by a Java StackOverflow exception. A remote attacker could exploit this by using a large depth of nested objects. **CVE-2022-24785 -** A directory traversal vulnerability exists in Moment.js as a result of the improper validation of user supplied input. An attacker could send a specially-crafted locale string containing "dot dot" sequences (/../) to switch arbitrary moment locale. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	All versions of IBM QRadar User Behavior Analytics prior to version 4.1.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6825139 https://www.ibm.com/support/pages/node/6825141

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.