



# Advisory Alert

Alert Number: AAA20220627 Date: June 27, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

## Overview

Product	Severity	Vulnerability
IBM	Critical	Remote Code Execution Vulnerability
IBM	Medium	Multiple Vulnerabilities

## Description

Affected Product	IBM
Severity	Critical
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2022-22963, CVE-2022-22965, CVE-2022-22950)
Description	<p>IBM QRadar SIEM is affected but not vulnerable to a remote code execution in Spring Framework (CVE-2022-22965) as it does not meet all of the following criteria: 1. JDK 9 or higher, 2. Apache Tomcat as the Servlet container, 3. Packaged as WAR (in contrast to a Spring Boot executable jar), 4. Spring-webmvc or spring-webflux dependency, 5. Spring Framework versions 5.3.0 to 5.3.17, 5.2.0 to 5.2.19, and older versions. QVM utilizes the Spring Framework to support our Java backed user interface. The fix includes Spring 5.3.18</p> <p>IBM highly recommends to apply necessary security fixes at earliest to avoid issues.</p>
Affected Products	QRadar / QRM / QVM / QRIF / QNI v7.3 QRadar / QRM / QVM / QRIF / QNI v7.4 QRadar / QRM / QVM / QRIF / QNI v7.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.ibm.com/support/pages/node/6598419">https://www.ibm.com/support/pages/node/6598419</a>

Affected Product	IBM
Severity	Medium
Affected Vulnerability	Multiple vulnerabilities (CVE-2020-14779, CVE-2020-14797, CVE-2021-35603, CVE-2021-35550, CVE-2021-35578, CVE-2021-35565, CVE-2022-21496, CVE-2022-21299, CVE-2020-14781, CVE-2020-14782)
Description	<p>IBM has released remediations to address multiple vulnerabilities that exist in the IBM Runtime Environment Java Version 8 that used by WebSphere eXtreme Scale product. Successful exploitation of these vulnerabilities could cause denial of service and sensitive information disclosure.</p> <p>IBM highly recommends to take necessary remediation steps to avoid issues.</p>
Affected Products	WebSphere Extreme Scale 8.6.1.0 – 8.6.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://www.ibm.com/support/pages/node/6598349">https://www.ibm.com/support/pages/node/6598349</a>

## 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.