



Advisory Alert

Alert Number: AAA20221206

Date: December 6, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	High, Medium, Low	Multiple Vulnerabilities
RedHat	Low	Denial of Service Vulnerability

Description

Affected Product	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42916, CVE-2022-32221, CVE-2022-35260, CVE-2022-42915, CVE-2022-37434, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208, CVE-2022-32205, CVE-2022-35252, CVE-2022-2097, CVE-2018-25032, CVE-2021-0091, CVE-2021-0092, CVE-2021-0093, CVE-2021-0099, CVE-2021-0103, CVE-2021-0107, CVE-2021-0111, CVE-2021-0114, CVE-2021-0115, CVE-2021-0116, CVE-2021-0117, CVE-2021-0118, CVE-2021-0119, CVE-2021-0124, CVE-2021-0125, CVE-2021-0156, CVE-2021-0127, CVE-2021-0145, CVE-2021-33120, CVE-2022-22476, CVE-2022-34165)
Description	<p>IBM has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of the most severe vulnerabilities could lead to security restriction bypass, privilege escalation, sensitive information disclosure, heap-based buffer overflow and denial of service.</p> <p>IBM highly recommends to apply the necessary security updates at your earliest to avoid issues.</p>
Affected Products	QRadar WinCollect Agent 10.0.0 - 10.1.0 All M6 Firmware versions before 7.1.0 All M5 Firmware versions before 9.0.0 IBM Spectrum Scale 5.1.0.0 - 5.1.2.6 IBM Spectrum Scale 5.1.3.0 - 5.1.5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6845359 https://www.ibm.com/support/pages/node/6845365 https://www.ibm.com/support/pages/node/6844721

Affected Product	RedHat
Severity	Low
Affected Vulnerability	Denial of Service Vulnerability (CVE-2022-2764)
Description	<p>Redhat has released a security update to address a denial of service vulnerability that exists in JBoss Enterprise Application Platform.</p> <p>CVE-2022-2764- A flaw found in Undertow with EJB invocations allows an attacker to generate a valid HTTP request and send it to the server on an established connection after removing the LAST_CHUNK from the bytes, causing a denial of service.</p> <p>Redhat recommends to apply the necessary security updates at your earliest to avoid issues.</p>
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:8793

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.