Advisory Alert

Alert Number: AAA20221027 **Date:** October 27, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
IBM	**High**	Denial Of Service Vulnerability
Redhat	**High**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-17571, CVE-2021-44832, CVE-2021-4104, CVE-2018-25032, CVE-2022-30126, CVE-2022-1271, CVE-2021-37404, CVE-2022-2047, CVE-2022-2048, CVE-2020-15522, CVE-2022-1729, CVE-2022-1966, CVE-2022-1552, CVE-2022-30973, CVE-2022-25169, CVE-2022-33879, CVE-2022-22968, CVE-2022-29885, CVE-2022-0492, CVE-2021-33036, CVE-2022-25762, CVE-2022-32250)
Description	IBM has released security updates addressing multiple critical vulnerabilities that exist in IBM QRadar SIEM. Exploitation of the most severe vulnerabilities cause arbitrary code execution, bypass security restrictions, Privilege escalation, and denial of service condition. IBM highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	IBM QRadar SIEM 7.4.0 - 7.4.3 Fix Pack 6 IBM QRadar SIEM 7.5.0 - 7.5.0 Update Pack 2 IBM QRadar SIEM 7.5.0 - 7.5.0 Update Package 3 IBM QRadar SIEM All SNMP Protocol versions before 7.5.0-QRADAR-PROTOCOL-SNMP-7.5-20220928225435 IBM QRadar SIEM All SNMP Protocol versions before 7.4.0-QRADAR-PROTOCOL-SNMP-7.4-20220928225439
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/blogs/psirt/security-bulletin-due-to-use-of-apache-log4j-ibm-qradar-siem-is-vulnerable-to-arbitrary-code-execution-cve-2019-17571-cve-2021-44832-cve-2021-4104/ https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-is-vulnerable-to-using-components-with-known-vulnerabilities-14/

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial Of Service Vulnerability (CVE-2022-37734)
Description	IBM has released a security update addressing a denial of service vulnerability that exist in the GraphQL Java library used by IBM WebSphere Application Server Liberty. The vulnerability exist due to an uncontrolled resource consumption flaw. An attacker can exploit this by sending a specially-crafted request using directive overloading, resulting in a denial of service condition IBM highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	IBM WebSphere Application Server Liberty 17.0.0.3 - 22.0.0.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6832094

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33193, CVE-2021-36160, CVE-2021-39275, CVE-2021-41524, CVE-2021-44224, CVE-2021-45960, CVE-2021-46143, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-23852, CVE-2022-23990, CVE-2022-25235, CVE-2022-25236, CVE-2022-25313, CVE-2022-25314, CVE-2022-25315)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in the Red Hat JBoss Core Services. Attackers can exploit these vulnerabilities to cause Integer overflow, stack exhaustion, arbitrary code execution, and system crash. Redhat highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services 1 for RHEL 7 x86_64 Red Hat JBoss Core Services Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:7143 https://access.redhat.com/errata/RHSA-2022:7144

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.