Advisory Alert

Alert Number: AAA20220607 **Date:** June 7, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	High	Denial of Service
Redhat	Medium	Multiple Vulnerabilities

Description

Affected Product	IBM
Severity	High
Affected Vulnerability	Denial of service (CVE-2021-35515, CVE-2021-35516, CVE-2021-36090, CVE-2021-35517)
Description	IBM has released security updates addressing denial of service that exists in their QRadar SIEM product. **CVE-2021-35515** - When reading a specially crafted 7Z archive, the construction of the list of codecs that decompress an entry can result in an infinite loop. This could be used to cause a denial of service attack against services that use the Compress' sevenz package. **CVE-2021-35516, CVE-2021-36090, CVE-2021-35517**- When reading a specially crafted 7Z,ZIP,TAR archive, Compress can be made to allocate large amounts of memory that finally lead to an out of memory error even for very small inputs. This could be used to cause a denial of service attack against services that use the Compress' sevenz package, ' zip package, ' tar package accordingly.
Affected Products	IBM QRadar SIEM v7.3 IBM QRadar SIEM v7.4 IBM QRadar SIEM v7.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/blogs/psirt/security-bulletin-apache-commons-as-used-by-ibm-qradar-siem-is-vulnerable-to-denial-of-service-cve-2021-35515-cve-2021-35516-cve-2021-36090-cve-2021-35517/

Affected Product	Redhat
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36518, CVE-2021-37136, CVE-2021-37137, CVE-2021-42392, CVE-2021-43797, CVE-2022-0084, CVE-2022-0853, CVE-2022-0866, CVE-2022-1319, CVE-2022-21299, CVE-2022-21363, CVE-2022-23221, CVE-2022-23437, CVE-2022-23913, CVE-2022-24785)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in their JBoss Enterprise Application. These flows could leads to denial of service, remote code execution, memory leakage, infinity loop and Path traversal vulnerabilities. Redhat recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 7 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-2022:4919 https://access.redhat.com/errata/RHSA-2022:4918 https://access.redhat.com/errata/RHSA-2022:4922

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.