Advisory Alert

Alert Number: AAA20230113 **Date:** January 13, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
RedHat	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**RedHat**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-4144, CVE-2022-3821, CVE-2022-2964, CVE-2022-4139, CVE-2022-35737, CVE-2022-2625,CVE-2022-46364)
Description	Redhat has released Security Updates addressing Multiple Vulnerabilities that exist in their products. Exploitation of the most severe vulnerabilities could cause code execution, Server-Side Request Forgery, privilege escalation, denial of service, and array-bounds overflow. Redhat recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 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-2023:0099 https://access.redhat.com/errata/RHSA-2023:0100 https://access.redhat.com/errata/RHSA-2023:0101 https://access.redhat.com/errata/RHSA-2023:0110 https://access.redhat.com/errata/RHSA-2023:0113 https://access.redhat.com/errata/RHSA-2023:0114 https://access.redhat.com/errata/RHSA-2023:0123 https://access.redhat.com/errata/RHSA-2023:0163 https://access.redhat.com/errata/RHSA-2023:0164

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.