Advisory Alert

Alert Number: AAA20221209 **Date:** December 9, 2022

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-2022-1292, CVE-2022-2068, CVE-2022-22721, CVE-2022-23943, CVE-2022-26377, CVE-2022-28330, CVE-2022-28614, CVE-2022-28615, CVE-2022-30522, CVE-2022-31813, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208, CVE-2022-32221, CVE-2022-35252, CVE-2022-37434, CVE-2022-40303, CVE-2022-40304, CVE-2022-40674, CVE-2022-42915, CVE-2022-42916, CVE-2022-28733)
Description	RedHat has released security updates addressing multiple vulnerabilities that exist in their packages and products. Exploitation of the most severe vulnerabilities could cause integer underflow, out of bound read/write, buffer overflow, denial of service, command injection, and HSTS bypass. RedHat highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le 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-2022:8900 https://access.redhat.com/errata/RHSA-2022:8840 https://access.redhat.com/errata/RHSA-2022:8841

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.