Advisory Alert

Alert Number: AAA20210319 **Date:** March 19, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
Xen	**High**	Denial Of Service

Description

Affected Product	Redhat
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-1983,CVE-2020-16092,CVE-2015-8011,CVE-2020-10722,CVE-2020-10723,CVE-2020-10724)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exists with multiple Redhat products. The most severe could cause buffer overflow vulnerability and Redhat highly recommends to apply necessary fixes at earliest to avoid issues.
Affected Products	Red Hat OpenStack 13 x86_64 Red Hat OpenStack for IBM Power 13 ppc64le Red Hat OpenStack Director Deployment Tools 13 x86_64 Red Hat OpenStack Director Deployment Tools for IBM Power LE 13 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2020-1983 https://access.redhat.com/security/cve/CVE-2020-16092 https://access.redhat.com/security/cve/CVE-2015-8011 https://access.redhat.com/security/cve/CVE-2020-10722 https://access.redhat.com/security/cve/CVE-2020-10723 https://access.redhat.com/security/cve/CVE-2020-10724

Affected Product	Xen
Severity	**High**
Affected Vulnerability	Denial of service (CVE-2021-28687)
Description	Xen project has released security updates addressing a denial of service vulnerability that exists in their products. Using this vulnerability a malicious user can crash the management daemon resulting in a system wide denial of service.
Affected Products	Xen versions 4.12 through 4.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	http://xenbits.xen.org/xsa/advisory-368.html

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.