Advisory Alert

Alert Number: AAA20210309 **Date:** March 9, 2021

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	**CVE-2021-22883 – High CVE-2021-22884 - Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	**CVE-2021-22883**: When too many connection attempts with an 'unknownProtocol' are established, a leak of file descriptors can occur leading to a potential denial of service. If no file descriptor limit is configured, then this can lead to excessive memory usage and cause the system to run out of memory. **CVE-2021-22884**: Node.js before 10.24.0, 12.21.0, 14.16.0, and 15.10.0 is vulnerable to DNS rebinding attacks as the whitelist includes “localhost6”. When “localhost6” is not present in /etc/hosts, it is just an ordinary domain that is resolved via DNS, i.e., over the network. If the attacker controls the victim's DNS server or can spoof its responses, the DNS rebinding protection can be bypassed by using the “localhost6” domain.
Affected Products	Red Hat Software Collections Red Hat Quay 3 Red Hat Enterprise Linux 8 Red Hat Enterprise Linux 8 Red Hat Enterprise Linux 8.1 Extended Update Support Red Hat Enterprise Linux 8.2 Extended Update Support Red Hat Enterprise Linux 8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2021-22884 https://access.redhat.com/security/cve/CVE-2021-22883

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.