Advisory Alert

Alert Number : AAA20200617 **Date :** June 17, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat Enterprise Linux	**High**	Kernel Memory Corruption

Description

Affected Product	**Redhat Enterprise Linux**
Severity	**High**
Affected Vulnerability	Kernel Memory Corruption (CVE-2020-12657)
Description	This vulnerability allows a local user who is able to access system memory to cause kernel memory corruption and possibly privilege escalation using a race condition in the IO scheduler
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.2 ppc64le Red Hat Enterprise Linux Server - TUS 8.2 x86_64 Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2020:2567 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12657

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.