Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 086 **16-June-2020**

Name: Red Hat Enterprise Linux Server kernel Security update

Affected Systems: Affects the following Linux versions:

- Red Hat Enterprise Linux Server – AUS & TUS 7.3 x86_64
- Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 7.3 ppc64le
- Red Hat Enterprise Linux Server - Update Services for SAP Solutions 7.3 x86_64

Summary:

A NULL pointer dereference flaw exists in the Linux kernel's SE-Linux subsystem which could allow a remote network user to crash the system kernel, resulting in a denial of service (DOS) condition.

Severity	**HIGH**
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:
https://access.redhat.com/errata/RHSA-2020:2277

Recommendations:

- Please visit following official link for the details on how to apply the update: https://access.redhat.com/articles/11258
- Updates are available on the section 'Updated Packages' at following official link: https://access.redhat.com/errata/RHSA-2020:2277
- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.
- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.
- Whenever required, access the system with minimal access rights and privileges.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.