Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 085 **30-May-2020**

Threat Classification: Remote Code Execution

Name: Apache Tomcat Remote Code Execution Vulnerability (CVE-2020-9484)

Affected Systems: Affects the following Apache Tomcat versions:

- Apache Tomcat 10.0.0-M1 to 10.0.0-M4
- Apache Tomcat 9.0.0.M1 to 9.0.34
- Apache Tomcat 8.5.0 to 8.5.54
- Apache Tomcat 7.0.0 to 7.0.103

Summary:

Due to improper validation of the de-serialized data, a remote attacker, if able to control the contents and name of a file on the server, may execute arbitrary code by sending a specifically crafted request.

Severity	HIGH
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:
https://access.redhat.com/security/cve/cve-2020-9484

Recommendations:

- Please visit following official link for complete documentation and fixing of the aforementioned vulnerability:
  https://tomcat.apache.org/security.html

- Users may configure the PersistenceManager with an appropriate value for 'sessionAttributeValueClassNameFilter' to ensure that only application provided attributes are serialized and de-serialized.

- 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.