



Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 095

30-July-2020

Threat Classification: Denial of Service (DoS)

Name: Apache Tomcat WebSocket Denial of Service Vulnerability (CVE-2020-13935)

Affected Systems: Affects the following Apache Tomcat versions:

- Apache Tomcat 10.0.0-M1 to 10.0.0-M6
- Apache Tomcat 9.0.0.M1 to 9.0.36
- Apache Tomcat 8.5.0 to 8.5.56
- Apache Tomcat 7.0.27 to 7.0.104

Summary:

The payload length in a WebSocket frame was not correctly validated in the above-mentioned Apache Tomcat versions. Invalid payload lengths could trigger an infinite loop and multiple requests of such payload lengths could lead to a denial of service (DoS).

Severity	HIGH
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:

<https://access.redhat.com/security/cve/cve-2020-13935>

Recommendations:

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