Alert Bulletin

Bulletin N.: 2024-40
Publication Date: 24/09/2024
Subject: Alert 2024-40 Critical Vulnerability in Apache Tomcat DoS CVE-2024-38286
Traffic Light Protocol (TLP): White

Affected Product(s):

- Apache Tomcat 9.0.13 – 9.0.89
- Apache Tomcat 10.1.0 M1 – 10.1.24
- Apache Tomcat 11.0.0 M1 – 11.0.0 M20

Description:

A critical vulnerability has been discovered in Apache Tomcat, affecting versions up to 9.0.89, 10.1.24, and 11.0.0-M20. This vulnerability, identified as CVE-2024-38286, is related to the TLS Handshake Handler component and allows for excessive resource consumption. The issue, classified under CWE-400 (Resource Exhaustion), arises from improper management of limited resources during the TLS handshake process, which can lead to memory exhaustion and impact service availability.