Advisory Alert

Alert Number: AAA20230523 **Date:** May 23, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Apache	**Medium**	Denial of Service vulnerability

Description

Affected Product	**Apache**
Severity	**Medium**
Affected Vulnerability	Denial of Service vulnerability (CVE-2023-28709)
Description	Apache has released a security update for A security vulnerability has been identified in Apache Tomcat, affecting multiple versions. This vulnerability, identified as CVE-2023-28709, exists due to an incomplete fix in the previous patch. If non-default HTTP connector settings are used, allowing the maxParameterCount to be reached via query string parameters, an attacker can exploit this by submitting a request with exactly maxParameterCount parameters in the query string. This can bypass the limit for uploaded request parts, potentially leading to a denial of service (DoS) attack. Apache recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Apache Tomcat 11.0.0-M2 to 11.0.0-M4 Apache Tomcat 10.1.5 to 10.1.7 Apache Tomcat 9.0.71 to 9.0.73 Apache Tomcat 8.5.85 to 8.5.87
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://lists.apache.org/thread/7wvxonzwb7k9hx9jt3q33cmy7j97jo3j

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.