Apache Tomcat Security Update for Remote Code Execution Vulnerability on Windows (CVE-2019-0232)

Background

A remote code execution (RCE) vulnerability (CVE-2019-0232) was found in Apache Tomcat, an open source Java web application server. When Tomcat runs on Windows Operating System (OS) with the "enableCmdLineArguments" enabled, its Common Gateway Interface (CGI) Servlet is found to be vulnerable to remote code execution (RCE) due to a flaw in how the Java Runtime Environment (JRE) passes command line arguments to the underlying OS. The CGI Servlet is turned off by default.

Since the CGI Servlet is disabled by default and its option enableCmdLineArguments is disabled by default in Tomcat 9.0.x, the remote code execution vulnerability has been rated as important and not critical.

In response to this vulnerability, the CGI Servlet enableCmdLineArguments option will now be disabled by default in all versions of Apache Tomcat.

Impact

Successful exploitation of the vulnerability could allow a remote attacker to execute arbitrary code on a targeted Windows server running an affected version of Apache Tomcat, which can lead to a malicious takeover of the entire system and result in a full compromise.

Vulnerable or affected Versions

The following versions of Tomcat running on Windows OS are vulnerable:

- Apache Tomcat 9.0.0.M1 to 9.0.17
- Apache Tomcat 8.5.0 to 8.5.39
- Apache Tomcat 7.0.0 to 7.0.93

Solution (Mitigation or Recommendations):

Rw-CSIRT is strongly recommending **users** and **IT administrators** to apply one of the following mitigations:

- Ensure the CGI Servlet initialisation parameter "enableCmdLineArguments" is set to false
- Upgrade to Apache Tomcat 9.0.18 or later when released
- Upgrade to Apache Tomcat 8.5.40 or later when released
- Upgrade to Apache Tomcat 7.0.93 or later when released

This announcement is being made before the releases are available as the change to fix this issue is obviously security related and The CGI option enableCmdLineArguments is disabled by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability).

System Administrators should immediately verify their installations, look out for and upgrade to the corresponding patched versions below at **http://tomcat.apache.org/** when released:

- Apache Tomcat 9.0.18
- Apache Tomcat 8.5.40
- Apache Tomcat 7.0.94

An alternative mitigation measure is to change the "enableCmdLineArguments" default value from "true" to "false".

Affected users should: contact Rw-CSIRT: Call **4045** or write to **security@risa.rw**

References:

http://tomcat.apache.org/security-9.html
http://tomcat.apache.org/security-8.html
http://tomcat.apache.org/security-7.html
https://gbhackers.com/apache-tomcat-security-vulnerability/
https://thehackernews.com/2019/04/apache-tomcat-security-flaw.html
https://www.csa.gov.sg/singcert/news/advisories-alerts/remote-code-execution-vulnerability-cve-2019-0232-in-apache-tomcat
http://mail-archives.us.apache.org/mod_mbox/www-announce/201904.mbox/%3C13d878ec-5d49-c348-48d4-25a6c81b9605%40apache.org%3E

National Computer Security and Incident Response Team (Rw-CSIRT) Mission

Rw-CSIRT mission is to build cyber-security capabilities to increase the capacity of "early **Detection**, **Prevention**, **Response** to incidents and **Reduce** Vulnerability" and raise cyber security awareness in public.