Apache Software Foundation (ASF) lanzó nuevas versiones de su servidor de aplicaciones Tomcat para abordar una grave vulnerabilidad de seguridad que podría permitir a un hacker remoto ejecutar código malicioso y tomar el control de un servidor.

Desarrollado por ASF, Apache Tomcat es un servidor web de código abierto y un sistema servlet que utiliza algunas especificaciones Java EE como Java Servlet, JavaServer Pages (JSP), Expression Language y WebSocket para proporcionar un entorno de servidor web HTTP «Java puro» para «Concepto de Java» ejecutable.

La vulnerabilidad de ejecución remota de código (CVE-2019-0232) reside en el Servlet de Interfaz de Puerta de Enlace Común (CGI) cuando se ejecuta en Windows con enableCMDLineArguments habilitado y se produce debido a un error en la forma en que el entorno de ejecución de Java (JRE) pasa los argumentos de la línea de comandos a Windows.

Debido a que el Servlet CGI está deshabilitado de forma predeterminada y su opción enableCmdLineArguments está deshabilitada de forma predeterminada en Tomcat 9.0.x, la vulnerabilidad de ejecución remota de código se calificó como importante y no crítica.

En respuesta a esta vulnerabilidad, la opción enableCmdLineArguments del Servlet CGI estará deshabilitada de forma predeterminada en todas las versiones de Apache Tomcat.

## Versiones de Tomcat afectadas

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

## Versiones de Tomcat que no resultaron afectadas

- Apache Tomcat 9.0.18 y posteriores
- Apache Tomcat 8.5.40 y posteriores
- Apache Tomcat 7.0.94 y posteriores

La explotación exitosa de la vulnerabilidad podría permitir a un atacante ejecutar un comando arbitrario en un servidor de Windows específico que ejecuta una versión afectada de Apache Tomcat, lo que resulta en un compromiso total.

La vulnerabilidad fue informada al equipo de seguridad de Apache Tomcat por un investigador de seguridad (no nombrado por la Fundación de Software Apache) el 3 de marzo de 2019 y se hizo pública el 10 de abril de 2019 luego de que ASF lanzara versiones actualizadas.

Esta vulnerabilidad de Apache se solucionó con el lanzamiento de Tomcat versió 9.0.19 (aunque el problema se solucionó en Apache Tomcat 9.0.18, el voto de lanzamiento para la versión 9.0.18 no se aprobó).

Por lo tanto, se recomienda a los administradores que actualicen el software lo más pronto posible. Si no te es posible aplicar los parches de inmediato, puedes asegurarte de que el valor enableCmdLineArguments predeterminado del parámetro de inicialización del Servlet CGI esté establecido en falso.