CVE-2019-0232

1. **OVERVIEW:**

Apache Tomcat has a vulnerability in the CGI Servlet which can be exploited to achieve remote code execution (RCE). This is only exploitable when running on Windows in a non-default configuration in conjunction with batch files. When enableCmdLineArguments is enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default.

1. **Behind the Scenes:**

In Windows, the main function for creating processes is the CreateProcess function. And in contrast to C API functions like execve, arguments are not passed separately as an array of strings but in a single command line. On the other side, the entry point function WinMain expects a single command line argument as well.

This circumstance requires the program to parse the command line itself for extracting the arguments. And although Windows provides a CommandLineToArgvW function and supports C and C++ API entry point functions where arguments are already parsed by the runtime and passed in a argc/argv style, the rules for quoting command line arguments with all their quirks can be quite confusing. And there is no definitive guide on how to quote properly, let alone something like a ArgvToCommandLineW function that does it for you. That’s why many do it wrong, as “Everyone quotes command line arguments the wrong way” by Daniel Colascione observes

If a process is started using ProcessBuilder, the arguments are passed to the static method start of ProcessImpl, which is a platform-dependent class. In the Windows implementation of ProcessImpl, the start method calls the private constructor of ProcessImpl, which creates the command line for the CreateProcess call.

1. **Summary:**

Command line parsing in Windows is not consistent and therefore the implementation of proper quoting of command line argument even less. This may allow the injection of additional arguments.

Additionally, since CreateProcess implicitly starts .bat and .cmd in a cmd.exe shell environment, even command injection may be possible.

As a sample, Java for Windows fails to properly quote command line arguments. Even with ProcessBuilder where arguments are passed as a list of strings:

Argument injection is possible by providing an argument containing further quoted arguments, e. g., '"arg 1" "arg 2" "arg 3"'.

On cmd.exe process command lines, a simple '&calc&' alone suffices.

Only within the most strictly mode, the VERIFICATION\_CMD\_BAT verification type, injection is not possible:

Legacy mode:

VERIFICATION\_LEGACY: There is no SecurityManager present and jdk.lang.Process.allowAmbiguousCommands is not explicitly set to false (no default set)

allows argument injection

allows command injection in cmd.exe calls (explicit or implicit)

Strict mode:

VERIFICATION\_CMD\_BAT: Most strictly mode, file ends with .bat or .cmd

does not allow argument injection

does not allow command injection in cmd.exe calls

VERIFICATION\_WIN32: File does not end with .bat or .cmd

allows argument injection

allows command injection in cmd.exe calls (explicit or implicit)

However, Java’s check for switching to the VERIFICATION\_CMD\_BAT mode can be circumvented by adding whitespace after the .bat or .cmd.

1. **Steps To Replicate:**
2. Install a Java Runtime Environment (JRE) in Windows.
3. Download a vulnerable version of Tomcat and extract.
4. Modify the conf\context.xml file on line 19, to enable privileged context:

<Context privileged="true">

1. Modify conf\web.xml to enable the CGI Servlet by removing the comments around line 387 as follows and adding the following parameters (enableCmdLineArguments is only needed for Tomcat 9):

<servlet><servlet-name>cgi</servlet-name>

<servlet-class>org.apache.catalina.servlets.CGIServlet</servlet-class>

<init-param>

<param-name>cgiPathPrefix</param-name>

<param-value>WEB-INF/cgi</param-value>

</init-param>

<init-param>

<param-name>executable</param-name>

<param-value></param-value>

</init-param>

<init-param>

<param-name>enableCmdLineArguments</param-name>

<param-value>true</param-value>

</init-param>

<load-on-startup>5</load-on-startup>

</servlet>

1. Enable the CGI servlet by removing comments around this – you also need to change the URL pattern to match the one in the previous step (“cgi”):

<servlet-mapping>

<servlet-name>cgi</servlet-name>

<url-pattern>/cgi/\*</url-pattern>

</servlet-mapping>

1. Create a folder for the CGI files:

mkdir webapps\ROOT\WEB-INF\cgi

1. Place the following text into a batch file located in “webapps\ROOT\WEB-INF\cgi\test.bat”

@echo off

echo Content-Type: text/plain

echo.

echo Hello, World!

1. Run Tomcat via the following command:

cd bin

catalina run

1. Trigger the following URLs and observe the dir command being run: <http://localhost:8080/cgi/test.bat?&dir>

Or run the attached PoC code.