CVE-2019-0232

Summary:

Apache Tomcat is vulnerable to Remote Code Execution(RCE) in non-default configuration in conjunction with batch files i.e. enableCmdLineArguments is set to True and CGI Servlet is enabled. Vulnerable versions are 7.0.0-7.0.93, 8.5.0-8.5.39 and 9.0.0-9.0.17.

The Vulnerability:

It's a High Critical Vulnerability allowing attackers to execute remote commands because of no input sanitization/filtering on the URL arguments. It is possible only when Common Gateway Interface(CGI) Servlets is enabled(which is disabled by default) and enableCmdLineArguments is set to True(which is default in versions < 9) and only windows OS are vulnerable.The CGI servlet parses URL parameters and translates them into command line arguments . There is no filtering done either by Tomcat or Windows JRE. When we pass *&* metacharacter in the URL parameter with a path of .bat/.cmd file, cmd.exe tries to execute the file, and treats *&* metacharacter as a command separator. So, if we pass any command after *&* metacharacter, it will get executed.

Exploit:

The vulnerability gets triggered when we pass any valid command in URL parameters after the *&* metacharacter. For triggering this, CGI Servlet must be enabled by modifying conf/web.xml file and adding the CGI Servlet parameters. enableCmdLineArguments are enabled by default in versions < 9. So, for versions 9.0.0-9.0.17, enableCmdLineArguments must also be added. Moreover, add the URL path of /cgi-vuln/ in servlet-mapping to match cgiPathPrefix. Create a sample batch file in the configured Path.

On running the server, we can easily exploit this vulnerability by passing URL parameters as : http://<VICTIM-IP>:<TOMCAT-PORT>/cgi-vuln/vuln.bat?&dir. Here, dir command gets executed.

In my exploit, I tried to get a reverse shell. This can be done by generating a simple reverse_shell.exe file(which can be done by msfvenom) which when executed by the victim, will connect back to us, giving us the shell access. For transferring the file, I base64 encoded the file, and transferred it to the victim(VM). I also transferred a vbscript which will base64 decode back the encoded file to the executable and run the reverse_shell.exe.

By default, Tomcat doesn't pass all environment variables from its parent process. Only variables set by Tomcat are passed. So, we need to run the full command path in order to execute any command otherwise we will get "not recognized or external command" as an error message.