Ghostcat Vulnerability Scanner (CVE-2020-1938) Report

✓ vuln.tomcat.com

Summary

Overall risk level:

High

Risk ratings:

High:	1
Medium:	0
Low:	0
Info:	0

Scan information:

Start time:	2020-03-12 16:54:20 UTC+02
Finish time:	2020-03-12 16:54:21 UTC+02
Scan duration:	1 sec
Tests performed:	1/1
Scan status:	Finished

Findings

Ghostcat (CVE-2020-1938) - Arbitrary File Read / Inclusion (port 8009)

We were able to read the contents of the file **WEB-INF/web.xml** from the web root of the target server:

```
<web-app xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://java.sun.com/xml/ns/javaee" xmlns:web="http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd" xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://java.sun.com/xml/ns/javaee/web-app_2_5.xsd" id="WebApp_ID" version="2.5">
  <display-name>online-store</display-name>
  <servlet>
    <description></description>
    <display-name>OnlineStoreStartup</display-name>
    <servlet-name>OnlineStoreStartup</servlet-name>
    <servlet-class>eastrip.servlet.Startup</servlet-class>
    <load-on-startup>1</load-on-startup>
  </servlet>
  <servlet-mapping>
    <servlet-name>OnlineStoreStartup</servlet-name>
    <url-pattern>/online-store</url-pattern>
  </servlet-mapping>
</web-app>
```

Details

Risk description:
The target Apache Tomcat server is vulnerable to an Arbitrary File Read / Inclusion vulnerability (aka Ghostcat - CVE-2020-1938) via its AJP Connector, which is reachable on port 8009.
An attacker is able to read any file from the web root directory (/webapps) of the Tomcat server, including configuration files (ex. WEB-INF/web.xml) and source code files (ex. index.jsp).

Furthermore, in certain cases when the web application allows users to upload files in the web root of the server, this vulnerability can also be used to include and execute those files, leading to Remote Code Execution.

Recommendation:
We recommend upgrading the Apache Tomcat server to the latest version, which is not affected by this vulnerability.

However, a workaround is to disable the AJP Connector if it is not used by your website. This can be done from the file **/conf/server.xml**. But if you do use the AJP Connector, another way to mitigate this vulnerability is to add the attribute **requiredSecret** to the Connector definition in the same file **/conf/server.xml**.

References:
https://nvd.nist.gov/vuln/detail/CVE-2020-1938
https://www.chaitin.cn/en/ghostcat.

Scan coverage information

List of tests performed (1/1)

- ✓ Scanning for Ghostcat CVE-2020-1938 vulnerability...

Scan parameters

Target:	vuln.tomcat.com
Port:	8009
File to read:	WEB-INF/web.xml