Generated Java and Scala Code Contains Local Information Disclosure Vulnerability

Moderate **wing328** published **GHSA-cqxr-xf2w-943w** on May 10, 2021

Package

org.openapitools:openapi-generator (Maven)

Affected versions	Patched versions
< 5.1.1	5.1.1

Description

Impact

This vulnerability impacts generated code. If this code was generated as a one-off occasion, not as a part of an automated CI/CD process, this code will remain vulnerable until fixed manually!

On Unix-Like systems, the system temporary directory is shared between all local users. When files/directories are created, the default `umask` settings for the process are respected. As a result, by default, most processes/apis will create files/directories with the permissions `-rw-r--r--` and `drwxr-xr-x` respectively, unless an API that explicitly sets safe file permissions is used.

This vulnerability exists due to the use of the JDK method `File.createTempFile`. This method creates an insecure temporary files that can leave application and system data vulnerable to exposure.

Auto-generated code (Java, Scala) that deals with uploading or downloading binary data through API endpoints will create insecure temporary files during the process. For example, if the API endpoint returns a PDF file, the auto-generated clients will first download the PDF into a insecure temporary file that can be read by anyone on the system.

Affected generators:

- Java
  - `okhttp-gson` (default library)

openapi-generator/modules/openapi-generator/src/main/resources/Java/libraries/okhttp-gson/ApiClient.mustache
Lines 1085 to 1088 in `d85f61f`

```
1085      if (tempFolderPath == null)
1086          return File.createTempFile(prefix, suffix);
1087      else
1088          return File.createTempFile(prefix, suffix, new File(tempFolderPath));
```

  - `jersey2`

openapi-generator/modules/openapi-generator/src/main/resources/Java/libraries/jersey2/ApiClient.mustache
Lines 1035 to 1038 in `d85f61f`

```
1035      if (tempFolderPath == null)
1036        return File.createTempFile(prefix, suffix);
1037      else
1038        return File.createTempFile(prefix, suffix, new File(tempFolderPath));
```

  - `resteasy`

openapi-generator/modules/openapi-generator/src/main/resources/Java/libraries/resteasy/ApiClient.mustache
Lines 604 to 607 in `d85f61f`

```
604      if (tempFolderPath == null)
605        return File.createTempFile(prefix, suffix);
606      else
607        return File.createTempFile(prefix, suffix, new File(tempFolderPath));
```

  - `retrofit2`

openapi-generator/modules/openapi-generator/src/main/resources/Java/libraries/retrofit2/play26/ApiClient.mustache
Lines 202 to 208 in `d85f61f`

```
202                     @Override
203                     public File convert(ResponseBody value) throws IOException {
204
205                         File file = File.createTempFile("retrofit-file", ".tmp");
206                         Files.write(Paths.get(file.getPath()), value.bytes());
207                         return file;
208                     }
```

- Scala
  - `scala-finch`

openapi-generator/modules/openapi-generator/src/main/resources/scala-finch/api.mustache
Lines 83 to 88 in `764a3b0`

```
83          private def bytesToFile(input: Array[Byte]): java.io.File = {
84            val file = File.createTempFile("tmp{{classname}}", null)
85            val output = new FileOutputStream(file)
86            output.write(input)
87            file
88          }
```

  - `scala-akka`

openapi-generator/modules/openapi-generator/src/main/resources/scala-akka-http-server/multipartDirectives.mustache
Lines 71 to 73 in `150e24d`

```
71        val tempFileFromFileInfo: FileInfo => File = {
72          file: FileInfo => File.createTempFile(file.fileName, ".tmp")
73        }
```

Patches

The issue has been patched by changing the generated code to use the JDK method `Files.createTempFile` and released in the v5.1.0 stable version.

References

#8787
#8791
#9348

This vulnerability has the same root cause as CVE-2021-21364 from the `swagger-api/swagger-codegen` project as this project and that one both share the same original source tree.
GHSA-hpv8-9rq5-hq7w

For more information

If you have any questions or comments about this advisory:

- Open an issue in OpenAPI Generator Github repo
- Email us at security@openapitools.org

Severity

Moderate 6.2 / 10

CVSS base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None
Availability	None

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVE ID

CVE-2021-21430

Weaknesses

CWE-377 CWE-378 CWE-379

Credits


JLLeitschuh