OpenAPI-Generator online generator: Local Privilege Escalation Vulnerability via System Temp Directory

Critical **wing328** published **GHSA-23x4-m842-fmwf** on May 10, 2021

Package

openapi-generator-online.jar (Maven)

Affected versions	Patched versions
< 5.1.0	5.1.0

Description

Impact

On Unix like systems, the system's temporary directory is shared between all users on that system. A collocated user can observe the process of creating a temporary sub directory in the shared temporary directory and race to complete the creation of the temporary subdirectory.

This vulnerability is local privilege escalation because the contents of the outputFolder can be appended to by an attacker. As such, code written to this directory, when executed can be attacker controlled.

openapi-generator-online creates insecure temporary folders with `File.createTempFile` during the code generation process. The insecure temporary folders store the auto-generated files which can be read and appended to by any users on the system.

Vulnerable Code

openapi-generator/modules/openapi-generator-online/src/main/java/org/openapitools/codegen/online/service/Generator.java
Lines 184 to 187 in c653051

```
184     File outputFolder = File.createTempFile("codegen-", "-tmp");
185     outputFolder.delete();
186     outputFolder.mkdir();
187     outputFolder.deleteOnExit();
```

This vulnerability exists due to a race condition between the deletion of the randomly generated temporary file and the creation of the temporary directory.

```
File outputFolder = File.createTempFile("codegen-", "-tmp"); // Attacker knows the full path of the file that will be generated
// delete the file that was created
outputFolder.delete(); // Attacker sees file is deleted and begins a race to create their own directory before the code generator
// and make a directory of the same name
// SECURITY VULNERABILITY: Race Condition! - Attacker beats the code generator and now owns this directory
outputFolder.mkdir();
```

Patches

The issue has been patched by changing the underlying logic to use `Files.createTempFile` and has been released in the v5.1.0 stable version.

References

#8788

This vulnerability has the same root cause as CVE-2021-21363 from the `swagger-api/swagger-codegen` project as this project and that one both share the same original source tree.
See: GHSA-pc22-3g76-gm6j

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

Critical 9.3 / 10

CVSS base metrics

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

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

CVE ID

CVE-2021-21428

Weaknesses

CWE-377 CWE-378 CWE-379

Credits

 JLLeitschuh