Information disclosure through temporary directory permissions

Moderate **big-guy** published **GHSA-fp8h-qmr5-j4c8** on Apr 9, 2021

Package

Gradle (Java)

Affected versions	Patched versions
<7.0	7.0

Description

Impact

Files created with open permissions in the system temporary directory can allow an attacker to access information downloaded by Gradle. Some builds could be vulnerable to a local information disclosure.

Remote files accessed through `TextResourceFactory` are downloaded into the system temporary directory first. Sensitive information contained in these files can be exposed to other local users on the same system.

If you do not use the `TextResourceFactory` API, you are not vulnerable.

What should you do?

Upgrade to Gradle 7.0

As of Gradle 7.0, uses of the system temporary directory have been moved to the Gradle User Home directory. By default, this directory is restricted to the user running the build.

Workarounds for older versions

Set a more restrictive umask that removes read access to other users. When files are created in the system temporary directory, they will not be accessible to other users.

If you are unable to change your system's umask, you can move the Java temporary directory by setting the System Property `java.io.tmpdir`. The new path needs to limit permissions to the build user only.

References

- Vulnerable code:

gradle/subprojects/core/src/main/java/org/gradle/api/internal/resources/ApiTextResourceAdapter.java
Lines 65 to 72 in ad8c7c9

```
65      public File asFile(String targetCharset) {
66          try {
67              File file = getWrappedTextResource().getFile();
68              if (file == null) {
69                  file = tempFileProvider.createTemporaryFile("wrappedInternalText", ".txt", "resource");
70                  Files.asCharSink(file, Charset.forName(targetCharset)).write(getWrappedTextResource().getText());
71                  return file;
72              }
```

- CWE-377: Insecure Temporary File

Questions?

- For security related issues, please email us at security@gradle.com.
- For non-security related issues, please open an issue on GitHub.

Severity

Moderate 4.0 / 10

CVSS base metrics

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

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

CVE ID

CVE-2021-29429

Weaknesses

CWE-377

Credits


big-guy


JLLeitschuh