Information Disclosure

Affecting com.google.guava:guava package, versions **[, 30.0-android) (30.0-android, 30.0-jre)**

INTRODUCED: 2 OCT 2020 CVE-2020-8908 CWE-200 Share

How to fix?

There is no fix for `com.google.guava:guava`. However, in version 30.0 and above, the vulnerable functionality has been deprecated. In oder to mitigate this vulnerability, upgrade for version 30.0 or higher and ensure your dependencies don't use the createTempFile or createTempFile methods.

Overview

com.google.guava:guava is a set of core libraries that includes new collection types (such as multimap and multiset,immutable collections, a graph library, functional types, an in-memory cache and more.

Affected versions of this package are vulnerable to Information Disclosure. The file permissions on the file created by `com.google.common.io.Files.createTempDir` allows an attacker running a malicious program co-resident on the same machine to steal secrets stored in this directory. This is because, by default, on unix-like operating systems the /tmp directory is shared between all users, so if the correct file permissions aren't set by the directory/file creator, the file becomes readable by all other users on that system.

PoC

```
File guavaTempDir = com.google.common.io.Files.createTempDir(); System.out.println("Guava Temp Dir: " +
guavaTempDir.getName()); runLS(guavaTempDir.getParentFile(), guavaTempDir); // Prints the file permissions
-> drwxr-xr-x File child = new File(guavaTempDir, "guava-child.txt"); child.createNewFile();
runLS(guavaTempDir, child); // Prints the file permissions -> -rw-r--r--
```

For Android developers, it is recommend choosing a temporary directory API provided by Android, such as `context.getCacheDir()`. For other Java developers, we recommend migrating to the Java 7 API `java.nio.file.Files.createTempDirectory()` which explicitly configures permissions of 700, or configuring the Java runtime's java.io.tmpdir system property to point to a location whose permissions are appropriately configured.

References

- GHSA Advisory
- GitHub Commit
- GitHub Issue

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low

See more

NVD 3.3 LOW

Red Hat 3.3 LOW

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk ID	SNYK-JAVA-COMGOOGLEGUAVA-1015415
Published	23 Oct 2020
Disclosed	2 Oct 2020
Credit	Jonathan Leitschuh

Report a new vulnerability | Found a mistake?

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.