# CVE Detail – CVE-2021-21290

Netty is an open-source, asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. In Netty before version 4.1.59.Final there is a vulnerability on Unix-like systems involving an insecure temp file. When netty's multipart decoders are used local information disclosure can occur via the local system temporary directory if temporary storing uploads on the disk is enabled. On unix-like systems, the temporary directory is shared between all user. As such, writing to this directory using APIs that do not explicitly set the file/directory permissions can lead to information disclosure. Of note, this does not impact modern MacOS Operating Systems. The method "File.createTempFile" on unix-like systems creates a random file, but, by default will create this file with the permissions "-rw-r--r--". Thus, if sensitive information is written to this file, other local users can read this information. This is the case in netty's "AbstractDiskHttpData" is vulnerable. This has been fixed in version 4.1.59.Final. As a workaround, one may specify your own "java.io.tmpdir" when you start the JVM or use "DefaultHttpDataFactory.setBaseDir(...)" to set the directory to something that is only readable by the current user.

## Threat-Mapped Scoring

Score: 3.75

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.02193

## CVSS Scoring

CVSS v3.1 Score: 6.2

Severity: MEDIUM

## Mapped CWE(s)

* CWE-378: Creation of Temporary File With Insecure Permissions
* CWE-379: Creation of Temporary File in Directory with Insecure Permissions
* CWE-668: Exposure of Resource to Wrong Sphere

## Affected Products

* cpe:2.3:a:netty:netty:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:quarkus:quarkus:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_corporate\_lending\_process\_management:14.2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_corporate\_lending\_process\_management:14.3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_corporate\_lending\_process\_management:14.5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_credit\_facilities\_process\_management:14.2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_credit\_facilities\_process\_management:14.3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_credit\_facilities\_process\_management:14.5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_trade\_finance\_process\_management:14.2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_trade\_finance\_process\_management:14.3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_trade\_finance\_process\_management:14.5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_brm\_-\_elastic\_charging\_engine:12.0.0.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_design\_studio:7.4.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_messaging\_server:8.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:nosql\_database:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:netapp:active\_iq\_unified\_manager:-:\*:\*:\*:\*:linux:\*:\*
* cpe:2.3:a:netapp:active\_iq\_unified\_manager:-:\*:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:netapp:cloud\_secure\_agent:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:netapp:snapcenter:-:\*:\*:\*:\*:\*:\*:\*