# CVE Detail – CVE-2022-24823

Netty is an open-source, asynchronous event-driven network application framework. The package `io.netty:netty-codec-http` prior to version 4.1.77.Final contains an insufficient fix for CVE-2021-21290. 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. This only impacts applications running on Java version 6 and lower. Additionally, this vulnerability impacts code running on Unix-like systems, and very old versions of Mac OSX and Windows as they all share the system temporary directory between all users. Version 4.1.77.Final contains a patch for this vulnerability. As a workaround, specify one's own `java.io.tmpdir` when starting the JVM or use DefaultHttpDataFactory.setBaseDir(...) to set the directory to something that is only readable by the current user.

## Threat-Mapped Scoring

Score: 2.55

Priority: P3 - Important (Medium)

## EPSS

EPSS Score: N/A

Percentile: 0.51554

## CVSS Scoring

CVSS v3.1 Score: 5.5

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:a:oracle:financial\_services\_crime\_and\_compliance\_management\_studio:8.0.8.2.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:financial\_services\_crime\_and\_compliance\_management\_studio:8.0.8.3.0:\*:\*:\*:\*:\*:\*:\*
* 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:oncommand\_workflow\_automation:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:netapp:snapcenter:-:\*:\*:\*:\*:\*:\*:\*