Local Information Disclosure Vulnerability in Netty on Unix-Like systems due temporary files for Java 6 and lower in io.netty:netty-codec-http

Moderate **normanmaurer** published **GHSA-269q-hmxg-m83q** on May 6

Package

netty-common (Maven)

Affected versions	Patched versions
<= 4.1.76.Final	4.1.77.Final

Description

Description

GHSA-5mcr-gq6c-3hq2 (CVE-2021-21290) contains an insufficient fix for the vulnerability identified.

Impact

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.

Vulnerability Details

To fix the vulnerability the code was changed to the following:

```
@SuppressJava6Requirement(reason = "Guarded by version check")
public static File createTempFile(String prefix, String suffix, File directory) throws IOExc
    if (javaVersion() >= 7) {
        if (directory == null) {
```

```
                return Files.createTempFile(prefix, suffix).toFile();
            }
            return Files.createTempFile(directory.toPath(), prefix, suffix).toFile();
        }
        if (directory == null) {
            return File.createTempFile(prefix, suffix);
        }
        File file = File.createTempFile(prefix, suffix, directory);
        // Try to adjust the perms, if this fails there is not much else we can do...
        file.setReadable(false, false);
        file.setReadable(true, true);
        return file;
    }
```

Unfortunately, this logic path was left vulnerable:

```
        if (directory == null) {
            return File.createTempFile(prefix, suffix);
        }
```

This file is still readable by all local users.

Patches

Update to 4.1.77.Final

Workarounds

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 or update to Java 7 or above.

References

- CWE-378: Creation of Temporary File With Insecure Permissions
- CWE-379: Creation of Temporary File in Directory with Insecure Permissions

For more information

If you have any questions or comments about this advisory:

Open an issue in netty

Severity

Moderate 5.5 / 10

CVSS base metrics

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

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

CVE ID

CVE-2022-24823

Weaknesses

CWE-378 CWE-379

Credits

 JLLeitschuh