WriteEntryToDirectory used for an archive extraction is vulnerable to partial path traversal.

High **adamhathcock** published **GHSA-jp7f-grcv-6mjf** on Sep 16, 2021

Package

 sharpcompress (NuGet)

Affected versions   Patched versions

<= 0.28.3   0.29

Description

SharpCompress recreates a hierarchy of directories under destinationDirectory if ExtractFullPath is set to true in options. In order to prevent extraction outside the destination directory the destinationFileName path is verified to begin with fullDestinationDirectoryPath. However it is not enforced that fullDestinationDirectoryPath ends with slash:

```
public static void WriteEntryToDirectory(IEntry entry,
                                         string destinationDirectory,
                                         ExtractionOptions? options,
                                         Action<string, ExtractionOptions?> write)
{
    string destinationFileName;
    string file = Path.GetFileName(entry.Key);
    string fullDestinationDirectoryPath = Path.GetFullPath(destinationDirectory);
...
        throw new ExtractionException("Entry is trying to write a file outside of the destination directory.");
}
```

If the destinationDirectory is not slash terminated like /home/user/dir it is possible to create a file with a name thats begins as the destination directory one level up from the directory, i.e. /home/user/dir.sh.

Impact

Because of the file name and destination directory constraints the arbitrary file creation impact is limited and depends on the use case.

Severity

High

CVE ID

CVE-2021-39208

Weaknesses

CWE-22

Credits

 JarLob