



CVE-2021-32842

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-32842
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-26 21:15:00 UTC
Updated	2022-02-07 19:09:00 UTC
Description	SharpZipLib (or #ziplib) is a Zip, GZip, Tar and BZip2 library. Starting version 1.0.0 and prior to version 1.3.3, a check was made to ensure that the file was not a directory. This check was bypassed by a path traversal attack using a sequence of backslashes followed by a dot and a backslash. This allowed an attacker to write to arbitrary files on the system.

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sharpziplib Project	Sharpziplib	All	All	All	All

References

Reference	Source
Release v1.3.3 · icsharpcode/SharpZipLib · GitHub	MISC
GHSL-2021-125: Path traversal in SharpZipLib - CVE-2021-32840, CVE-2021-32841, CVE-2021-32842 GitHub Security Lab	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[591178](#) Phoenix Contact FL Network Manager Path Traversal Vulnerability (CVE-2021-32840,CVE-2021-32842)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report