



CVE-2018-1002206

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

Summary

CVE	CVE-2018-1002206
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-25 17:29:00 UTC
Updated	2019-10-09 23:32:00 UTC
Description	SharpCompress before 0.21.0 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a ../ (dot d

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
GitHub - snyk/zip-slip-vulnerability: Zip Slip Vulnerability (Arbitrary file write through archive extraction)	MISC
fix: prevent extracting archived files outside of target path by odinn1984 · Pull Request #374 · adamhathcock/sharpcompress · GitHub	CON
Zip Slip Vulnerability Snyk	MISC
Arbitrary File Write via Archive Extraction (Zip Slip) in sharpcompress Snyk	MISC
Merge pull request #374 from odinn1984/feat/fail_on_outside_target_files · adamhathcock/sharpcompress@42b1205 · GitHub	CON
CVE Program record	CVE.
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[983791](#) Dotnet (nuget) Security Update for sharpcompress (GHSA-fxh6-w476-hgr4)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)