



CVE-2022-44900

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

Summary

CVE	CVE-2022-44900
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-12-06 20:15:00 UTC
Updated	2022-12-09 14:28:00 UTC
Description	A directory traversal vulnerability in the SevenZipFile.extractall() function of the python library py7zr v0.20.0 and earlier allow

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Py7zr Project	Py7zr	All	All	All	All

References

Reference	Source	Link	Tags
py7zr 0.20.0 Directory Traversal ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE-2022-44900: path traversal vulnerability in py7zr less on sec	MISC	lessonsec.com	
Fix sanity check for path traversal attack · miurahr/py7zr@1bb43f1 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[183387](#) Debian Security Update for py7zr (CVE-2022-44900)

[6000553](#) Debian Security Update for py7zr (DSA 5652-1)

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