



# CVE-2022-29072

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-29072
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-04-15 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:45:00 UTC
<b>Description</b>	** DISPUTED ** 7-Zip through 21.07 on Windows allows privilege escalation and command execution when a file with the

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	7-zip	7-zip	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

## References

### Reference

Please update your browser

7-Zip up to 21.07 on Windows allows privilege escalation and command execution | Hacker News

7-Zip 21.07 Code Execution / Privilege Escalation ≈ Packet Storm

GitHub - kagancapar/CVE-2022-29072: 7-Zip through 21.07 on Windows allows privilege escalation and command execution when a file with

SourceForge.net: Log In to SourceForge.net

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[376545](#) 7-Zip Privilege Escalation and Command Execution Vulnerability (Zero Day)

© [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](#)