



CVE-2022-4772

Published on: Not Yet Published

Last Modified on: 01/05/2023 08:21:00 PM UTC

CVE-2022-4772

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Widoco](#) from [Widoco Project](#) contain the following vulnerability:

A vulnerability was found in Widoco and classified as critical. Affected by this issue is the function unZiplt of the file `src/main/java/widoco/WidocoUtils.java`. The manipulation leads to path traversal. It is possible to launch the attack on the local host. The name of the patch is `f2279b76827f32190adfa9bd5229b7d5a147fa92`. It is recommended to apply a patch to fix this issue. VDB-216914 is the identifier assigned to this vulnerability.

CVE-2022-4772 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
vuln-fix: Zip Slip Vulnerability - dgarijo/Widoco@f2279b7 · GitHub	github.com text/html	MISC github.com/dgarijo/Widoco/commit/f2279b76827f32190adfa9bd5229b7d5a147fa92
CVE-2022-4772 Widoco WidocoUtils.java unZiplt path traversal (ID 551)	vuldb.com text/html	MISC vuldb.com/?id.216914
CVE-2022-4772 Widoco WidocoUtils.java unZiplt path traversal (ID 551)	vuldb.com text/html	MISC vuldb.com/?ctiid.216914
[SECURITY] Fix Zip Slip Vulnerability by github.com MISC github.com/dgarijo/Widoco/pull/551		

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Widoco Project	Widoco	All	All	All	All
cpe:2.3:a:widoco_project:widoco:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-4772 : A vulnerability was found in Widoco and classified as critical. Affected by this issue is the funct... twitter.com/i/web/status/1...	2022-12-27 23:05:22
 /r/netcve	CVE-2022-4772	2022-12-27 23:38:20

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023  |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)