

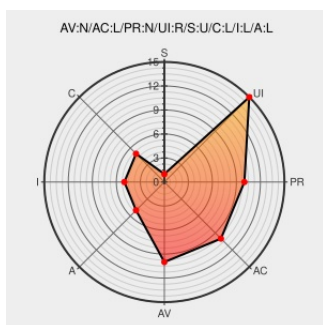


CVE-2022-3724

Published on: Not Yet Published

Last Modified on: 06/27/2023 08:44:00 PM UTC

CVE-2022-3724

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

Certain versions of [Windows](#) from [Microsoft](#) contain the following vulnerability:

Crash in the USB HID protocol dissector in Wireshark 3.6.0 to 3.6.8 allows denial of service via packet injection or crafted capture file on Windows

CVE-2022-3724 has been assigned by [cve@gitlab.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Wireshark Foundation](#) - **Wireshark** version $\geq 3.6.0$, $< 3.6.8$

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
2022/CVE-2022-3724.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-3724.json
Wireshark · wnpa-sec-2022-08 · USB-HID dissector crash on Windows	www.wireshark.org text/html	MISC www.wireshark.org/security/wnpa-sec-2022-08.html
Crash in USB-HID dissector on Windows (#18384) · Issues · Wireshark Foundation / wireshark · GitLab	gitlab.com text/html	MISC gitlab.com/wireshark/wireshark/-/issues/18384

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
Operating System	Microsoft	Windows	-	All	All	All
Application	Wireshark	Wireshark	All	All	All	All
cpe:2.3:o:microsoft:windows:-:*****:						
cpe:2.3:a:wireshark:wireshark:*****:						

Discovery Credit

TODO

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-3724 : Crash in the USB HID protocol dissector in Wireshark 3.6.0 to 3.6.8 allows denial of service via pa... twitter.com/i/web/status/1...	2022-12-09 18:05:09
 /r/netcve	CVE-2022-3724	2022-12-09 18:45:33

[← 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](#)