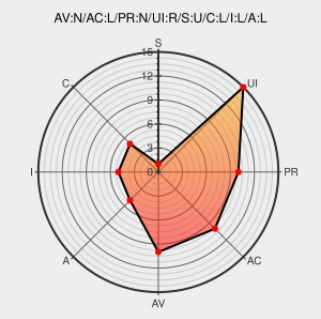
CVE-2022-3724

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 **>=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

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→