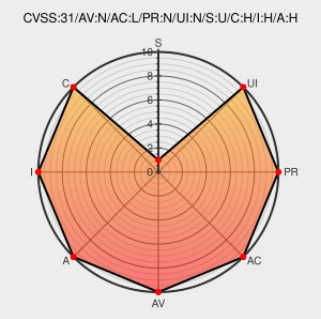
CVE-2023-46555

Published on: Not Yet Published

Last Modified on: 10/27/2023 10:00:00 PM UTC

CVE-2023-46555

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of X2000r from Totolink contain the following vulnerability:

TOTOLINK X2000R Gh v1.0.0-B20230221.0948.web was discovered to contain a stack overflow via the function formPortFw.

CVE-2023-46555 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
No Description Provided	totolink.cn	MISC totolink.cn/home/menu/detail.html?menu_listtpl=download&id=85&ids=36
0、Vulnerability Introduction	github.com text/plain	MISC github.com/XYIYM/Digging/blob/main/TOTOLINK/X2000R/3/1.md

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
Hardware	Totolink	X2000r	-	All	All	All
Operating System	Totolink	X2000r Firmware	1.0.0-b20230221.0948	All	All	All

cpe:2.3:h:totolink:x2000r:-:*:*:*:*:*:*:*:

cpe:2.3:o:totolink:x2000r_firmware:1.0.0-b20230221.0948:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→