



CVE-2022-30326

Published on: Not Yet Published

Last Modified on: 06/27/2022 07:12:00 PM UTC

CVE-2022-30326

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

Certain versions of [Tew-831dr](#) from [Trendnet](#) contain the following vulnerability:

An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The network pre-shared key field on the web interface is vulnerable to XSS. An attacker can use a simple XSS payload to crash the basic.config page of the web interface.

CVE-2022-30326 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
NCC Group Research – Making the world safer and more secure	research.nccgroup.com text/html	MISC research.nccgroup.com/?research=Technical+advisories
Technical Advisory – Multiple Vulnerabilities in Trendnet TEW-831DR WiFi Router (CVE-2022-30325, CVE-2022-30326, CVE-	research.nccgroup.com text/html	MISC research.nccgroup.com/2022/06/10/technical-

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	Trendnet	Tew-831dr	-	All	All	All
Operating System	Trendnet	Tew-831dr Firmware	1.0_601.130.1.1356	All	All	All
cpe:2.3:h:trendnet:tew-831dr:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:trendnet:tew-831dr_firmware:1.0_601.130.1.1356:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@NCCGroupInfosec	Technical Advisory – Multiple Vulnerabilities in Trendnet TEW-831DR WiFi Router (CVE-2022-30325, CVE-2022-30326, CV... twitter.com/i/web/status/1...	2022-06-10 18:36:20
@buaqbot	Technical Advisory – Multiple Vulnerabilities in Trendnet TEW-831DR WiFi Router (CVE-2022-30325, CVE-2022-30326, CV... twitter.com/i/web/status/1...	2022-06-10 19:21:17
@CVEreport	CVE-2022-30326 : An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The network pre-shared key fi... twitter.com/i/web/status/1...	2022-06-16 23:05:39
@threatmeter	CVE-2022-30326 An issue was found on TRENDnet TEW-831DR 1.0 601.130.1.1356 devices. The network pre-shared key fiel... twitter.com/i/web/status/1...	2022-06-17 07:10:03
@circl_lu	research.nccgroup.com/2022/06/10/tec... Technical Advisory – Multiple Vulnerabilities in Trendnet TEW-831DR WiFi Router (CVE-2022-... twitter.com/i/web/status/1...	2022-06-17 09:18:02
@Har_sia	CVE-2022-30326 har-sia.info/CVE-2022-30326... #HarsiaInfo	2022-06-17 23:02:11
/r/netcve	CVE-2022-30326	2022-06-17 00:38:46

[← Previous ID](#)

[Next ID →](#)

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](#)