CVE-2022-43636

Published on: Not Yet Published

Last Modified on: 04/07/2023 02:16:00 PM UTC

CVE-2022-43636

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

Certain versions of Tl-wr940n from Tp-link contain the following vulnerability:

This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of TP-Link TL-WR940N 6_211111 3.20.1(US) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of sufficient randomness in the sequnce numbers used for session managment. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-18334.

CVE-2022-43636 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **TP-Link** - **TL-WR940N** version **6_211111 3.20.1(US)**

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
ZDI-22-1614 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-22-1614/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Tl-wr940n	-	All	All	All
Operating System	Tp-link	Tl-wr940n Firmware	6_211111_3.20.1	All	All	All

cpe:2.3:h:tp-link:tl-wr940n:-:*:*:*:*:*:*:*:

cpe:2.3:o:tp-link:tl-wr940n_firmware:6_211111_3.20.1:*:*:*:*:*:*:*:

Discovery Credit

ExLuck

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-43636	2023-03-29 20:38:19

← Previous ID

Next ID→