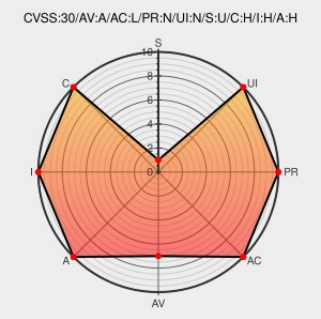
CVE-2022-24354

Published on: Not Yet Published

Last Modified on: 02/28/2022 06:59:00 PM UTC

CVE-2022-24354

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



Certain versions of Ac1750 from Tp-link contain the following vulnerability:

This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link AC1750 prior to 1.1.4 Build 20211022 rel.59103(5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the NetUSB.ko module. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15835.

CVE-2022-24354 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **TP-Link** - **AC1750** version **prior to 1.1.4 Build 20211022 rel.59103(5553)**

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

CVSS2 Score: 8.3 - HIGH

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
ZDI-22-264 | Zero Day Initiative	www.zerodayinitiative.com text/html	MISC www.zerodayinitiative.com/advisories/ZDI-22-264/

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	Ac1750	-	All	All	All
Operating System	Tp-link	Ac1750 Firmware	All	All	All	All

cpe:2.3:h:tp-link:ac1750:-:*:*:*:*:*:*:*:

cpe:2.3:o:tp-link:ac1750_firmware:*:*:*:*:*:*:*:*:

Discovery Credit

Axel '0vercl0k' Souchet from https://doar-e.github.io/

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-24354 : This vulnerability allows network-adjacent attackers to execute arbitrary code on affected install… twitter.com/i/web/status/1…	2022-02-28 19:29:51
/r/netcve	CVE-2022-24354	2022-02-28 20:38:46

← Previous ID

Next ID→