



# CVE-2022-24354

Published on: Not Yet Published

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

## CVE-2022-24354

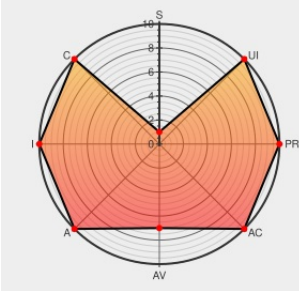
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:30/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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	<a href="http://www.zerodayinitiative.com">www.zerodayinitiative.com</a> <a href="#">text/html</a>	 MISC <a href="http://www.zerodayinitiative.com/advisories/ZDI-22-264/">www.zerodayinitiative.com/advisories/ZDI-22-264/</a>
----------------------------------	---	---

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](mailto: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 	<a href="#">Tp-link</a>	<a href="#">Ac1750</a>	-	All	All	All
Operating System	<a href="#">Tp-link</a>	<a href="#">Ac1750 Firmware</a>	All	All	All	All
<input type="text" value="cpe:2.3:h:tp-link:ac1750:-:*:*:*:*:*:*"/>						
<input type="text" value="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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2022-02-28 19:29:51
 /r/netcve	<a href="#">CVE-2022-24354</a>	2022-02-28 20:38:46

[← Previous ID](#) [Next ID →](#)

© CVE.report 2023   | Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)