



CVE-2023-34832

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-34832
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-16 18:15:00 UTC
Updated	2023-06-23 21:19:00 UTC
Description	TP-Link Archer AX10(EU)_V1.2_230220 was discovered to contain a buffer overflow via the function FUN_131e8 - 0x132B

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Archer Ax10	1.2	All	All	All
Operating System	Tp-link	Archer Ax10 Firmware	230220	All	All	All

References

Reference	Source	Link	Tags
CVE-2023-34832 : Buffer Overflow in TP-Link Archer AX10(EU)_V1.2_230220 · GitHub	MISC	gist.github.com	
TP-Link Archer AX10(EU)_V1.2_230220 Buffer Overflow ≈ Packet Storm	MISC	packetstormsecurity.com	
Archer	MISC	archer.com	
TP-Link Canada - WiFi Networking Equipment for Home & Business	MISC	tp-link.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)