



Denial-of-Service Vulnerability in UPnP Component of TP Link's TL-WR841N

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

Summary

CVE	CVE-2026-3622
State	PUBLISHED
Assigner	TPLink
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-26 21:17:09 UTC
Updated	2026-03-31 19:09:04 UTC
Description	The vulnerability exists in the UPnP component of TL-WR841N v14, where improper input validation leads to an out-of-bou

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from f23511db-6c3e-4e32-a477-6aa17d310630

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000460000 probability, percentile 0.141030000 (date 2026-04-01)

Problem Types: CWE-125 | CWE-125 CWE-125 Out-of-bounds read

Version	Source	Type	Score	Severity	Vector
4.0	f23511db-6c3e-4e32-a477-6aa17d310630	Secondary	7.1	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:
4.0	CNA	CVSS	7.1	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	TP-link	TL-wr841n	14	All	All	All
Operating System	TP-link	TL-wr841n Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-Link Systems Inc.	TL-WR841N V14	affected 0.9.1 4.19 custom	Linux

References

Reference	Source	Link	Tags
www.tp-link.com/us/support/download/tl-wr841n/v14	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
www.tp-link.com/us/support/faq/5033	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Vendor Advisory
www.tp-link.com/en/support/download/tl-wr841n/v14	f23511db-6c3e-4e32-a477-6aa17d310630	www.tp-link.com	Product
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Md Sharafatullah Zomadder, Professor Rahamatullah Khondoker, Dept. of Business Informatics, THM University of Applied Sciences, Friedberg, Germany (en)

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](#).

CVE.report and Source URL Uptime Status status.cve.report