



TP-Link TL-WR720N All Versions CSRF via Administrative Interfaces

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

Summary

CVE	CVE-2018-25321
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-17 13:16:43 UTC
Updated	2026-05-17 13:16:43 UTC
Description	TP-Link TL-WR720N wireless router contains a cross-site request forgery vulnerability that allows attackers to perform unau

Risk And Classification

Primary CVSS: v4.0 5.3 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/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

Problem Types: CWE-352 | CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/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
4.0	CNA	CVSS	5.3	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/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
3.1	disclosure@vulncheck.com	Primary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality: None

Integrity: Low

Availability: None

Sub Conf.: Low

Sub Integrity: Low

Sub Availability: Low

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:L/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MS:C:X/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: Low

User Interaction: None

Scope: Unchanged

Confidentiality: None

Integrity: Low

Availability: None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	TP-link	TL-WR720NMbps Wireless N Router	affected V1_130719	Not specified

References

Reference	Source	Link	Tags
www.exploit-db.com/exploits/44335	disclosure@vulncheck.com	www.exploit-db.com	

static.tp-link.com/resources/software/TL-WR720N_V1_130719.zip	disclosure@vulncheck.com	static.tp-link.com	
www.tp-link.com	disclosure@vulncheck.com	www.tp-link.com	
www.vulncheck.com/advisories/tp-link-tl-wr720n-all-versions-csrf-via-administra...	disclosure@vulncheck.com	www.vulncheck.com	
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

Vendor Comments And Credit

Discovery Credit

CNA: Mans van Someren (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](#).

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

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