



CVE-2015-3035

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

Summary

CVE	CVE-2015-3035
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-22 01:59:02 UTC
Updated	2026-04-21 17:05:04 UTC
Description	Directory traversal vulnerability in TP-LINK Archer C5 (1.2) with firmware before 150317, C7 (2.0) with firmware before 150317

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

EPSS: 0.931270000 probability, percentile 0.997970000 (date 2026-04-22)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-22 | n/a | CWE-22 CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	7.8	HIGH	AV:N/AC:L/Au:N/C:I/N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:C/I:N/A:N

CISA Known Exploited Vulnerability

Vendor	TP-Link
Product	Multiple Archer Devices
Name	TP-Link Multiple Archer Devices Directory Traversal Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2015-3035

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Tp-link	Archer C5	1.20	All	All	All
Operating System	Tp-link	Archer C5 Firmware	All	All	All	All
Hardware	Tp-link	TI-wr740n	5	All	All	All
Operating System	Tp-link	TI-wr740n Firmware	All	All	All	All
Hardware	Tp-link	TI-wr741nd	5	All	All	All

Operating System	Tp-link	TI-wr741nd Firmware	All	All	All	All
Hardware	Tp-link	TI-wr841n	9	All	All	All
Operating System	Tp-link	TI-wr841n Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Download for TL-WR841N V9 - Welcome to TP-LINK	af854
Download for Archer C7 V2 - Welcome to TP-LINK	af854
Download for TL-WDR3500 V1 - Welcome to TP-LINK	af854
Full Disclosure: SEC Consult SA-20150410-0 :: Unauthenticated Local File Disclosure in multiple TP-LINK products (CVE-2015-3035)	af854
SecurityFocus	af854
Multiple TP-LINK Products CVE-2015-3035 Directory Traversal Vulnerability	af854
Download for TL-WR741ND V5 - Welcome to TP-LINK	af854
Download for TL-WDR3600 V1 - Welcome to TP-LINK	af854
Download for Archer C9 V1 - Welcome to TP-LINK	af854
Download for TL-WDR4300 V1 - Welcome to TP-LINK	af854
Download for TL-WR841ND V9 - Welcome to TP-LINK	af854
Download for Archer C5 V1.20 - Welcome to TP-LINK	af854
Download for TL-WR740N V5 - Welcome to TP-LINK	af854
Download for Archer C8 V1 - Welcome to TP-LINK	af854
Vulnerability Lab - SEC Consult	af854
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c
TP-LINK Local File Disclosure ≈ Packet Storm	af854
CVE Program record	CVE
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-25T00:00:00.000Z	CVE-2015-3035 added to CISA KEV

Legacy QID Mappings

731277 TP-Link Router Directory Traversal Vulnerability

© [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](#)