



Totolink A8000R cstecgi.cgi setLanguageCfg missing authentication

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

Summary

CVE	CVE-2026-5676
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-06 19:16:30 UTC
Updated	2026-04-07 13:20:11 UTC
Description	A vulnerability was identified in Totolink A8000R 5.9c.681_B20180413. This issue affects the function setLanguageCfg of t

Risk And Classification

Primary CVSS: v4.0 6.9 MEDIUM from cna@vulldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/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: 0.000770000 probability, percentile 0.229340000 (date 2026-04-07)

Problem Types: CWE-287 | CWE-306 | CWE-306 Missing Authentication | CWE-287 Improper Authentication

Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vulldb.com	Primary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:W/RC:R
3.0	CNA	DECLARED	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:W/RC:R
2.0	cna@vulldb.com	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:W/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low
Attack Requirements
None
Privileges Required
None
User Interaction
None
Confidentiality
Low
Integrity
Low
Availability
Low
Sub Conf.
None
Sub Integrity
None
Sub Availability
None
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/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
Low
Integrity
Low
Availability
Low
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

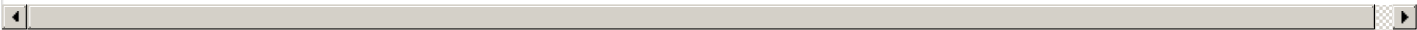
Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:W/RC:R



Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Totolink	A8000R	affected 5.9c.681_B20180413	Not specified

References

Reference	Source	Link	Tags
vuldb.com/submit/792433	cna@vuldb.com	vuldb.com	
vuldb.com/vuln/355503	cna@vuldb.com	vuldb.com	
github.com/skeetabc/CVE-TOTOLINK-A800R/blob/main/vuln1_auth_bypass.md	cna@vuldb.com	github.com	
www.totolink.net	cna@vuldb.com	www.totolink.net	
vuldb.com/vuln/355503/cti	cna@vuldb.com	vuldb.com	
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: skeet (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-06T00:00:00.000Z	Advisory disclosed

CNA	2026-04-06T02:00:00.000Z	VulDB entry created
CNA	2026-04-06T11:43:13.000Z	VulDB entry last update
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](#)