WDR201A WiFi Extender Stack-Based Buffer Overflow via firewall.cgi

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-41927
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 20:16:19 UTC
Updated	2026-05-05 19:47:31 UTC
Description	WDR201A WiFi Extender (HW V2.1, FW LFMZX28040922V1.02) contains a stack-based buffer overflow vulnerability in the

Risk And Classification

Primary CVSS: v4.0 8.3 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000420000 probability, percentile 0.125500000 (date 2026-05-05)

Problem Types: CWE-121 | CWE-121 CWE-121: Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.3	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA
4.0	CNA	CVSS	8.3	HIGH	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

Low

Integrity

Low

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Shenzhen Yipu Commercial And Trading Co. Ltd	WDR201A WiFi Extender	affected 1.02 semver	Not specified

References

Reference	Source	Link
mstreet97.github.io/security-research/iot/vulnerability-disclosure/ai-assisted-re...	disclosure@vulncheck.com	mstreet97.github.io
www.made-in-china.com/showroom/yeapook	disclosure@vulncheck.com	www.made-in-china.cor
www.vulncheck.com/advisories/wdr201a-wifi-extender-stack-based-buffer-overflow-...	disclosure@vulncheck.com	www.vulncheck.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Daniele Berardinelli (en)

CNA: Matteo Strada (en)

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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