



WDR201A WiFi Extender OS Command Injection via adm.cgi (reboot_time)

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

Summary

CVE	CVE-2026-41925
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 an OS command injection vulnerability in the ad

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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: 0.004520000 probability, percentile 0.637450000 (date 2026-05-05)

Problem Types: CWE-78 | CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (CWE-78)

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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 v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None
Confidentiality
High
Integrity
High
Availability
High
Sub Conf.
None
Sub Integrity
None
Sub Availability
None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/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



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.vulncheck.com/advisories/wdr201a-wifi-extender-os-command-injection-via-adm...	disclosure@vulncheck.com	www.vulncheck.com
www.made-in-china.com/showroom/yeapook	disclosure@vulncheck.com	www.made-in-china.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Matteo Strada (en)

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

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