

CVE-2024-12987

DrayTek Vigor Routers OS Command Injection Vulnerability

CISA KEV since May 15, 2025

Actively exploited

A vulnerability, which was classified as critical, was found in DrayTek Vigor2960 and Vigor300B 1.5.1.4. Affected is an unknown function of the file /cgi-bin/mainfunction.cgi/apmcfupload of the component Web Management Interface. The manipulation of the argument session leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.5.1.5 is able to address this issue. It is recommended to upgrade the affected component.

EVRS 84 / ₁₀₀ Urgent priority	CVSS V4.0 6.9 Medium · NVD	EPSS 0.982 99.91st percentile · FIRST	CISA DEADLINE Jun 5, 2025 KEV since 2025 · listed over a year
---	---	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.982 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.9	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
vigor300b firmware	1.5.1.4	no fixed version listed	NVD
vigor2960 firmware	1.5.1.4	no fixed version listed	NVD
vigor300b	—	no fixed version listed	NVD
vigor2960	—	no fixed version listed	NVD

Sources

Vendor guidance	netsecfish.notion.site/Command-Injection-in-apmcfgupload-endpoint-for-DrayTek-Gateway-Devices-1676b683e67c8040b7f1f0ffe29ce18f?pvs=4	Additional guidance	vuldb.com/?id.289380
Additional guidance	vuldb.com/?submit.468795	fw.draytek.com.tw	fw.draytek.com.tw/Vigor2960/Firmware/v1.5.1.5/DrayTek_Vigor2960_V1.5.1.5_01release-note.pdf
fw.draytek.com.tw	fw.draytek.com.tw/Vigor300B/Firmware/v1.5.1.5/DrayTek_Vigor300B_V1.5.1.5_01release-note.pdf	fw.draytek.com.tw	fw.draytek.com.tw/Vigor3900/Firmware/v1.5.1.5/DrayTek_Vigor3900_V1.5.1.5_01release-note.pdf
NVD	nvd.nist.gov/vuln/detail/CVE-2024-12987	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-51246	Current data	evulnable.com/vulnerability-management/cve/CVE-2024-12987

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.