

CVE-2024-40890

Zyxel DSL CPE OS Command Injection Vulnerability

CISA KEV since Feb 11, 2025

Actively exploited

****UNSUPPORTED WHEN ASSIGNED**** A post-authentication command injection vulnerability in the CGI program of the legacy DSL CPE Zyxel VMG4325-B10A firmware version 1.00(AAFR.4)C0_20170615 could allow an authenticated attacker to execute operating system (OS) commands on an affected device by sending a crafted HTTP POST request.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.207 97.5th percentile · FIRST	CISA DEADLINE Mar 4, 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	0.207 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: The impacted product could be end-of-life (EoL) and/or end-of-service (EoS). Users should discontinue product utilization if a current mitigation is unavailable.

Basis: CISA KEV required action

Affected and fixed versions · 19 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
vmg1312-b10a firmware	—	no fixed version listed	NVD
vmg1312-b10b firmware	—	no fixed version listed	NVD
vmg1312-b10e firmware	—	no fixed version listed	NVD
vmg3312-b10a firmware	—	no fixed version listed	NVD
vmg3313-b10a firmware	—	no fixed version listed	NVD
vmg3926-b10b firmware	—	no fixed version listed	NVD
vmg4325-b10a firmware	—	no fixed version listed	NVD
vmg4380-b10a firmware	—	no fixed version listed	NVD

Sources

Vendor guidance		github.com/advisories/GHSA-r9jg-gp7p-hp34	Additional guidance	zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-and-insecure-default-credentials-vulnerabilities-in-certain-legacy-dsl-cpe-02-04-2025
zyxel.com	zyxel.com/service-provider/global/en/security-advisories/zyxel-security-advisory-command-injection-insecure-in-certain-legacy-dsl-cpe-02-04-2025		NVD	nvd.nist.gov/vuln/detail/CVE-2024-40890
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog		ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2024-38809
Current data	evulnable.com/vulnerability-management/cve/CVE-2024-40890			

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