

CVE-2017-6884

Zyxel EMG2926 Routers Command Injection Vulnerability

CISA KEV since Sep 18, 2023

Actively exploited

Ransomware use known

A command injection vulnerability was discovered on the Zyxel EMG2926 home router with firmware V1.00(AAQT.4)b8. The vulnerability is located in the diagnostic tools, specifically the nslookup function. A malicious user may exploit numerous vectors to execute arbitrary commands on the router, such as the ping_ip parameter to the expert/maintenance/diagnostic/nslookup URI.

EVRS 75_{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.330 98.4th percentile · FIRST	CISA DEADLINE Oct 9, 2023 KEV since 2023 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.330 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: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
emg2926 firmware	v1.00\(\aaqt.4\)b8	no fixed version listed	NVD
emg2926	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-x6r5-p9fx-6346

zyxel.com zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-vulnerability-in-emg2926-q10a-ethernet-cpe,
<https://www.zyxelguard.com/ZyXel-EOL.asp>

NVD nvd.nist.gov/vuln/detail/CVE-2017-6884
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-15938

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2017-6884

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