

CVE-2016-10174

NETGEAR WNR2000v5 Router Buffer Overflow Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

The NETGEAR WNR2000v5 router contains a buffer overflow in the hidden_lang_avi parameter when invoking the URL / apply.cgi?/lang_check.html. This buffer overflow can be exploited by an unauthenticated attacker to achieve remote code execution.

EVRS 83 _{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.833 99.68th percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · 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	On the CISA KEV catalog for over two years
☒ EPSS	0.833 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 48 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
d6100 firmware	—	no fixed version listed	NVD
d7000 firmware	—	no fixed version listed	NVD
d7800 firmware	—	no fixed version listed	NVD
jnr1010v2 firmware	—	no fixed version listed	NVD
jnr3300 firmware	—	no fixed version listed	NVD
jwnr2010v5 firmware	—	no fixed version listed	NVD
r2000 firmware	—	no fixed version listed	NVD
r6100 firmware	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-rgmj-9q73-5phf	NVD	nvd.nist.gov/vuln/detail/CVE-2016-10174
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-1361
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-10174		

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