

CVE-2017-6862

NETGEAR Multiple Devices Buffer Overflow Vulnerability

CISA KEV since Jun 8, 2022

Actively exploited

NETGEAR WNR2000v3 devices before 1.1.2.14, WNR2000v4 devices before 1.0.0.66, and WNR2000v5 devices before 1.0.0.42 allow authentication bypass and remote code execution via a buffer overflow that uses a parameter in the administration webapp. The NETGEAR ID is PSV-2016-0261.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.457 98.8th percentile · FIRST	CISA DEADLINE Jun 22, 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	0.457 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
wnr2000 firmware	< 1.0.0.42 < 1.0.0.66 < 1.1.2.14	1.0.0.42 · 1.0.0.66 · 1.1.2.14	NVD
wnr2000	v5 v4 v3	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-xjjj-92c2-q84f

Additional guidance kb.netgear.com/000038542/Security-Advisory-for-Unauthenticated-Remote-Code-Execution-on-Some-Routers-PSV-2016-0261

NVD nvd.nist.gov/vuln/detail/CVE-2017-6862

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-15916

Current data evulnable.com/vulnerability-management/cve/CVE-2017-6862

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