

CVE-2016-1555

NETGEAR Multiple WAP Devices Command Injection Vulnerability

Exigent

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

(1) boardData102.php, (2) boardData103.php, (3) boardDataJP.php, (4) boardDataNA.php, and (5) boardDataWW.php in Netgear WN604 before 3.3.3 and WN802Tv2, WNAP210v2, WNAP320, WNDAP350, WNDAP360, and WNDAP660 before 3.5.5.0 allow remote attackers to execute arbitrary commands.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.983 99.92nd 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	0.983 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 6 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
wnap320 firmware	≤ 3.0.5.0	after 3.0.5.0	NVD
wndap350 firmware	≤ 3.0.5.0	after 3.0.5.0	NVD
wndap360 firmware	≤ 3.0.5.0	after 3.0.5.0	NVD
wndap210v2 firmware	≤ 3.0.5.0	after 3.0.5.0	NVD
wn604 firmware	≤ 3.3.2	after 3.3.2	NVD
wndap660 firmware	≤ 3.0.5.0	after 3.0.5.0	NVD
wn802tv2 firmware	≤ 3.0.5.0	no fixed version listed	NVD
wnap320	—	no fixed version listed	NVD

Sources

Vendor guidance	kb.netgear.com/30480/CVE-2016-1555-Notification?cid=wmt_netgear_organic	NVD	nvd.nist.gov/vuln/detail/CVE-2016-1555
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-2650
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-1555		

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