

CVE-2017-5521

NETGEAR Multiple Devices Exposure of Sensitive Information Vulnerability

CISA KEV since Sep 8, 2022

Actively exploited

Public exploit module (Metasploit)

An issue was discovered on NETGEAR R8500, R8300, R7000, R6400, R7300, R7100LG, R6300v2, WNDR3400v3, WNR3500Lv2, R6250, R6700, R6900, and R8000 devices. They are prone to password disclosure via simple crafted requests to the web management server. The bug is exploitable remotely if the remote management option is set, and can also be exploited given access to the router over LAN or WLAN.

EVRS 82/100 Urgent priority	CVSS V3.1 8.1 High · NVD	EPSS 0.894 99.79th percentile · FIRST	CISA DEADLINE Sep 29, 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	0.894 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions. If the affected device has since entered end-of-life, it should be disconnected if still in use.

Basis: CISA KEV required action

When trying to access the web panel, a user is asked to authenticate; if the authentication is canceled and password recovery is not enabled, the user is redirected to a page that exposes a password recovery token. If a user supplies the correct token to the page /passwordrecovered.cgi?id=TOKEN (and password recovery is not enabled), they will receive the admin password for the router. If password recovery is set the exploit will fail, as it will ask the user for the recovery questions that were previously set when enabling that feature. This is persistent (even after disabling the recovery option, the exploit will fail) because the router will ask for the security questions.

Affected and fixed versions · 18 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
r6200 firmware	1.0.1.56 1.0.43	no fixed version listed	NVD
r6300 firmware	1.0.2.78 1.0.58	no fixed version listed	NVD
vegn2610 firmware	1.0.0.36	no fixed version listed	NVD
ac1450 firmware	1.0.0.34 10.0.16	no fixed version listed	NVD
wnr1000v3 firmware	1.0.2.68 60.0.93	no fixed version listed	NVD
wndr3700v3 firmware	1.0.0.40 1.0.32	no fixed version listed	NVD
wndr4000 firmware	1.0.2.4 9.1.86	no fixed version listed	NVD
wndr4500 firmware	1.0.1.44 1.0.73	no fixed version listed	NVD



Sources

Vendor guidance github.com/advisories/GHSA-6c9f-r56h-g5xf

NVD nvd.nist.gov/vuln/detail/CVE-2017-5521

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2017-14625

kb.netgear.com kb.netgear.com/30632/Web-GUI-Password-Recovery-and-Exposure-Security-Vulnerability

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

Current data evulnable.com/vulnerability-management/cve/CVE-2017-5521

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