

CVE-2016-6277

NETGEAR Multiple Routers Remote Code Execution Vulnerability

CISA KEV since Mar 7, 2022

Actively exploited

Public exploit module (Metasploit)

NETGEAR R6250 before 1.0.4.6.Beta, R6400 before 1.0.1.18.Beta, R6700 before 1.0.1.14.Beta, R6900, R7000 before 1.0.7.6.Beta, R7100LG before 1.0.0.28.Beta, R7300DST before 1.0.0.46.Beta, R7900 before 1.0.1.8.Beta, R8000 before 1.0.3.26.Beta, D6220, D6400, D7000, and possibly other routers allow remote attackers to execute arbitrary commands via shell metacharacters in the path info to cgi-bin/.

EVRS

86/100

Immediate priority

CVSS V3.1

8.8

High · NVD

EPSS

0.998

99.96th percentile · FIRST

CISA DEADLINE

Sep 7, 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	0.998 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

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

Basis: CISA KEV required action

Affected and fixed versions · 14 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
d6220 firmware	≤ 1.0.0.22	after 1.0.0.22	NVD
d6400 firmware	≤ 1.0.0.56	after 1.0.0.56	NVD
r6250 firmware	≤ 1.0.4.6_10.1.12	after 1.0.4.6_10.1.12	NVD
r6400 firmware	≤ 1.0.1.18	after 1.0.1.18	NVD
r6700 firmware	≤ 1.0.1.14	after 1.0.1.14	NVD
r6900 firmware	≤ 1.0.1.14	after 1.0.1.14	NVD
r7000 firmware	≤ 1.0.7.2_1.1.93	no fixed version listed	NVD
r7100lg firmware	≤ 1.0.0.28	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-pxpc-qfm6-www4	NVD	nvd.nist.gov/vuln/detail/CVE-2016-6277
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-7207
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-6277		

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