

CVE-2019-16920

D-Link Multiple Routers Command Injection Vulnerability

Exigent

CISA KEV since Mar 25, 2022

Actively exploited

Unauthenticated remote code execution occurs in D-Link products such as DIR-655C, DIR-866L, DIR-652, and DHP-1565. The issue occurs when the attacker sends an arbitrary input to a "PingTest" device common gateway interface that could lead to common injection. An attacker who successfully triggers the command injection could achieve full system compromise. Later, it was independently found that these are also affected: DIR-855L, DAP-1533, DIR-862L, DIR-615, DIR-835, and DIR-825.

EVRS 87/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.99th 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	0.999 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: The impacted product is end-of-life and should be disconnected if still in use.

Basis: CISA KEV required action

Affected and fixed versions · 12 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
dir-655 firmware	≤ 3.02b05	after 3.02b05	NVD
dir-866l firmware	≤ 1.03b04	after 1.03b04	NVD
dir-652 firmware	—	no fixed version listed	NVD
dhp-1565 firmware	≤ 1.01	after 1.01	NVD
dir-855l firmware	—	no fixed version listed	NVD
dap-1533 firmware	—	no fixed version listed	NVD
dir-862l firmware	—	no fixed version listed	NVD
dir-615 firmware	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-5p5j-jvxx-68mp	NVD	nvd.nist.gov/vuln/detail/CVE-2019-16920
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	europa.eu/enisa/eu-vulnerability/EUVD-2019-7414
Current data	evulnable.com/vulnerability-management/cve/CVE-2019-16920		

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