

CVE-2020-9377

D-Link DIR-610 Devices Remote Command Execution

CISA KEV since Mar 25, 2022

Actively exploited

D-Link DIR-610 devices allow Remote Command Execution via the cmd parameter to command.php. NOTE: This vulnerability only affects products that are no longer supported by the maintainer

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.213 97.6th 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	0.213 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
dir-610 firmware	–	no fixed version listed	NVD
dir-610	–	no fixed version listed	NVD

Sources

Vendor guidance	gist.github.com/GouveaHeitor/131557f9de7d571f118f59805df852dc	Additional guidance	supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10182
NVD	nvd.nist.gov/vuln/detail/CVE-2020-9377	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2020-30198	Current data	evulnable.com/vulnerability-management/cve/CVE-2020-9377

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