

CVE-2011-4723

D-Link DIR-300 Router Cleartext Storage of a Password Vulnerability

CISA KEV since Sep 8, 2022

Actively exploited

The D-Link DIR-300 router stores cleartext passwords, which allows context-dependent attackers to obtain sensitive information via unspecified vectors.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 5.7 Medium · NVD	EPSS 0.031 87.5th 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	0.031 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 5.7	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source**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-300 firmware	–	no fixed version listed	NVD
dir-300	–	no fixed version listed	NVD

Sources

Vendor guidance cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2011-4723**NVD** nvd.nist.gov/vuln/detail/CVE-2011-4723**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2011-4641**dlink.com** dlink.com/uk/en/support/product/dir-300-wireless-g-router**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**Current data** evulnable.com/vulnerability-management/cve/CVE-2011-4723

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