

CVE-2018-6530

D-Link Multiple Routers OS Command Injection Vulnerability

Exigent

CISA KEV since Sep 8, 2022

Actively exploited

Ransomware use known

OS command injection vulnerability in soap.cgi (soapcgi_main in cgibin) in D-Link DIR-880L DIR-880L_REVA_FIRMWARE_PATCH_1.08B04 and previous versions, DIR-868L DIR868LA1_FW112b04 and previous versions, DIR-65L DIR-865L_REVA_FIRMWARE_PATCH_1.08.B01 and previous versions, and DIR-860L DIR860LA1_FW110b04 and previous versions allows remote attackers to execute arbitrary OS commands via the service parameter.

EVRs

93/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.967

99.89th 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.967 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 vendor D-Link published an advisory stating the fix under CVE-2018-20114 properly patches KEV entry CVE-2018-6530. If the device is still supported, apply updates per vendor instructions. If the affected device has since entered its end-of-life, it should be disconnected if still in use.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
dir-860l firmware	≤ 1.10b04	after 1.10b04	NVD
dir-865l firmware	≤ 1.08b01	after 1.08b01	NVD
dir-868l firmware	≤ 1.12b04	after 1.12b04	NVD
dir-880l firmware	≤ 1.08b04	after 1.08b04	NVD
dir-860l	a1	no fixed version listed	NVD
dir-865l	a1	no fixed version listed	NVD
dir-868l	a1	no fixed version listed	NVD
dir-880l	a1	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-j95f-33m4-87jf**supportannouncement.us.dlink.com** supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10105**NVD** nvd.nist.gov/vuln/detail/CVE-2018-6530**CISA KEV****ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2018-18282**Current data**evulnable.com/vulnerability-management/cve/CVE-2018-6530

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