

CVE-2015-2051

D-Link DIR-645 Router Remote Code Execution Vulnerability

CISA KEV since Feb 10, 2022

Actively exploited

Public exploit module (Metasploit)

The D-Link DIR-645 Wired/Wireless Router Rev. Ax with firmware 1.04b12 and earlier allows remote attackers to execute arbitrary commands via a GetDeviceSettings action to the HNAP interface.

EVRS 85 /100 Immediate priority	CVSS V3.1 8.8 High · NVD	EPSS 0.971 99.89th percentile · FIRST	CISA DEADLINE Aug 10, 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	0.971 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: 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-645 firmware	< 1.05b01	1.05b01	NVD
dir-645	a1	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-x629-5xff-w7qg

Additional guidance supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10282

NVD nvd.nist.gov/vuln/detail/CVE-2015-2051

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2015-2164

Current data evulnable.com/vulnerability-management/cve/CVE-2015-2051

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