

CVE-2015-1187

D-Link and TRENDnet Multiple Devices Remote Code Execution Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

Public exploit module (Metasploit)

The ping tool in multiple D-Link and TRENDnet devices allow remote attackers to execute arbitrary code via the ping_addr parameter to ping.ccp.

EVRS 82 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.829 99.67th 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	0.829 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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 · 22 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
dir-626l firmware	1.04	no fixed version listed	NVD
dir-636l firmware	1.04	no fixed version listed	NVD
dir-808l firmware	1.03	no fixed version listed	NVD
dir-810l firmware	1.01 2.02	no fixed version listed	NVD
dir-820l firmware	1.02 1.05 2.01	no fixed version listed	NVD
dir-826l firmware	1.00	no fixed version listed	NVD
dir-830l firmware	1.00	no fixed version listed	NVD
dir-836l firmware	1.01	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-2cvq-m957-r86c	NVD	nvd.nist.gov/vuln/detail/CVE-2015-1187
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	europa.eu/enisa/eu-vulnerability/EUVD-2015-1329
Current data	evulnable.com/vulnerability-management/cve/CVE-2015-1187		

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