

CVE-2020-25506

D-Link DNS-320 Device Command Injection Vulnerability

Exigent

CISA KEV since Nov 3, 2021

Actively exploited

D-Link DNS-320 FW v2.06B01 Revision Ax is affected by command injection in the system_mgr.cgi component, which can lead to remote arbitrary code execution.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.999 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: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
dns-320 firmware	2.06b01	no fixed version listed	NVD
dns-320	ax	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-vfrw-4wr4-4c85

Additional guidance supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10183

NVD nvd.nist.gov/vuln/detail/CVE-2020-25506

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

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-18191

Current data evulnable.com/vulnerability-management/cve/CVE-2020-25506

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