# D-Link DIR-825M formVpnConfigSetup sub_4151FC buffer overflow

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2026-7288 |
| **State** | PUBLISHED |
| **Assigner** | VulDB |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2026-04-28 15:16:37 UTC |
| **Updated** | 2026-04-30 13:27:19 UTC |
| **Description** | A vulnerability has been found in D-Link DIR-825M 1.1.12. This vulnerability affects the function sub_4151FC of the file /boa |

## Risk And Classification

**Primary CVSS:** v4.0 7.4 HIGH from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000330000 probability, percentile 0.095020000 (date 2026-05-05)

**Problem Types:** CWE-119 | CWE-120 | CWE-120 Buffer Overflow | CWE-119 Memory Corruption

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 4.0 | cna@vuldb.com | Secondary | 7.4 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/C... |
| 4.0 | CNA | DECLARED | 8.7 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P |
| 3.1 | cna@vuldb.com | Primary | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | CNA | DECLARED | 8.8 | HIGH | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R |
| 3.0 | CNA | DECLARED | 8.8 | HIGH | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R |
| 2.0 | cna@vuldb.com | Secondary | 9 | | AV:N/AC:L/Au:S/C:C/I:C/A:C |
| 2.0 | CNA | DECLARED | 9 | | AV:N/AC:L/Au:S/C:C/I:C/A:C/E:POC/RL:ND/RC:UR |

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Dlink | Dir-825m | - | All | All | All |
| Operating System | Dlink | Dir-825m Firmware | 1.1.12 | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | D-Link | DIR-825M | affected 1.1.12 | Not specified |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| vuldb.com/vuln/359946 | cna@vuldb.com | vuldb.com | Third Party Advisory, VDB Entry |
| github.com/Kiciot/cve/issues/2 | cna@vuldb.com | github.com | Exploit, Third Party Advisory |
| vuldb.com/vuln/359946/cti | cna@vuldb.com | vuldb.com | Permissions Required, VDB Entry |
| www.dlink.com | cna@vuldb.com | www.dlink.com | Product |
| vuldb.com/submit/803024 | cna@vuldb.com | vuldb.com | Third Party Advisory, VDB Entry |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

## Vendor Comments And Credit

Discovery Credit

**CNA:** kiciot (VulDB User) (en)

CNA: Kicist (VulDB User) (en)

## Additional Advisory Data

| Source | Time | Event |
|---|---|---|
| CNA | 2026-04-28T00:00:00.000Z | Advisory disclosed |
| CNA | 2026-04-28T02:00:00.000Z | VulDB entry created |
| CNA | 2026-04-28T11:50:37.000Z | VulDB entry last update |

There are currently no legacy QID mappings associated with this CVE.