VDB-356570 · CVE-2026-6014 · EUVD-2026-21310

# D-LINK DIR-513 1.10 POST REQUEST /GOFORM/FORMADVANCESETUP WEBPAGE BUFFER OVERFLOW

| CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score |
|---|---|---|
| 8.0 | $0-$5k | 2.64- |

## Summary

A vulnerability was found in D-Link DIR-513 1.10 and classified as critical. Impacted is the function `formAdvanceSetup` of the file */goform/formAdvanceSetup* of the component *POST Request Handler*. Such manipulation of the argument *webpage* leads to buffer overflow. This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability is referenced as CVE-2026-6014. It is possible to launch the attack remotely. Furthermore, an exploit is available.

## Details

A vulnerability was found in D-Link DIR-513 1.10. It has been rated as critical. Affected by this issue is the function `formAdvanceSetup` of the file */goform/formAdvanceSetup* of the component *POST Request Handler*. The manipulation of the argument `webpage` with an unknown input leads to a buffer overflow vulnerability. Using CWE to declare the problem leads to CWE-120. The product copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow. Impacted is confidentiality, integrity, and availability.

The advisory is available at lavender-bicycle-a5a.notion.site. This vulnerability is handled as CVE-2026-6014. The exploitation is known to be easy. The attack may be launched remotely. Technical details as well as a public exploit are known. The structure of the vulnerability defines a possible price range of USD $0-$5k at the moment (estimation calculated on 04/10/2026).

The exploit is available at lavender-bicycle-a5a.notion.site. It is declared as proof-of-concept.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-21310).

## Product

### Type

- Router Operating System

### Vendor

- D-Link

### Name

- DIR-513

### Version

- 1.10

### License

- commercial

### Support

- end of life

### Website

- Vendor: https://www.dlink.com/

## CPE 2.3

- 🔒

## CPE 2.2

- 🔒

## CVSSv4

**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

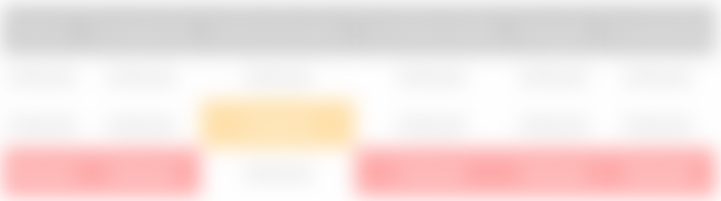
## CVSSv3

**VulDB Meta Base Score**: 8.8
**VulDB Meta Temp Score**: 8.0

**VulDB Base Score**: 8.8

**VulDB Temp Score**: 8.0
**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

## CVSSv2



**VulDB Base Score**: 🔒
**VulDB Temp Score**: 🔒
**VulDB Reliability**: 🔍

## Exploiting

**Class**: Buffer overflow
**CWE**: CWE-120 / CWE-119
**CAPEC**: 🔒
**ATT&CK**: 🔒

**Physical**: No
**Local**: No
**Remote**: Yes

**Availability**: 🔒
**Access**: Public
**Status**: Proof-of-Concept
**Download**: 🔒
**Price Prediction**: 🔍
**Current Price Estimation**: 🔒

## Threat Intelligence

**Interest**: 🔍
**Active Actors**: 🔍
**Active APT Groups**: 🔍

## Countermeasures

**Recommended**: no mitigation known
**Status**: 🔍

**0-Day Time**: 🔒

## Timeline

| | | |
|---|---|---|
| **04/09/2026** | | Advisory disclosed |
| **04/09/2026** | +0 days | VulDB entry created |
| **04/10/2026** | +1 days | VulDB entry last update |

## Sources

**Vendor**: dlink.com

**Advisory**: lavender-bicycle-a5a.notion.site
**Status**: Not defined

**CVE**: CVE-2026-6014 (🔒)
**GCVE (CVE)**: GCVE-0-2026-6014
**GCVE (VulDB)**: GCVE-100-356570
**EUVD**: 🔒
**scip Labs**: https://www.scip.ch/en/?labs.20161013

## Entry

**Created**: 04/09/2026 04:41 PM
**Updated**: 04/10/2026 08:52 AM
**Changes**: 04/09/2026 04:41 PM (59), 04/10/2026 08:52 AM (1)
**Complete**: 🔍
**Submitter**: wxhwxhwxh_mie
**Cache ID**: 172:CC3:179

## Submit

### Accepted

- Submit #791860: D-Link DIR-513 D-Link DIR-513 A2 1.10 Buffer Overflow (by wxhwxhwxh_mie)

## Discussion

No comments yet. Languages: en.

Please log in to comment.