VDB-356263 · CVE-2026-5815 · GCVE-100-356263

D-LINK DIR-645 1.01/1.02/1.03 /CGI-BIN/HEDWIG.CGI HEDWIGCGI_MAIN STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.0	$0-$5k	2.97

Summary

A vulnerability was found in D-Link DIR-645 1.01/1.02/1.03. It has been classified as critical. The affected element is the function `hedwigcgi_main` of the file */cgi-bin/hedwig.cgi*. This manipulation causes stack-based overflow. This vulnerability only affects products that are no longer supported by the maintainer. This vulnerability appears as CVE-2026-5815. The attack may be initiated remotely. In addition, an exploit is available.

Details

A vulnerability was found in D-Link DIR-645 1.01/1.02/1.03. It has been declared as critical. Affected by this vulnerability is the function `hedwigcgi_main` of the file */cgi-bin/hedwig.cgi*. The manipulation with an unknown input leads to a stack-based overflow vulnerability. The CWE definition for the vulnerability is CWE-121. A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function). As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-5815. The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known. The pricing for an exploit might be around USD $0-$5k at the moment (estimation calculated on 04/08/2026).

It is possible to download the exploit at github.com. 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.

Product

Type

- Router Operating System

Vendor

- D-Link

Name

- DIR-645

Version

- 1.01
- 1.02
- 1.03

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: Stack-based overflow
CWE: CWE-121 / 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

04/08/2026		Advisory disclosed
04/08/2026	+0 days	VulDB entry created
04/08/2026	+0 days	VulDB entry last update

Sources

Vendor: dlink.com

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5815 (🔒)
GCVE (CVE): GCVE-0-2026-5815
GCVE (VulDB): GCVE-100-356263
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/08/2026 05:35 PM
Changes: 04/08/2026 05:35 PM (57)
Complete: 🔍
Submitter: Pers1st
Cache ID: 172:0C0:179

Submit

Accepted

- Submit #788298: D-Link DIR-645 1.01–1.03 Stack-based Buffer Overflow (by Pers1st)

Discussion

No comments yet. Languages: en.

Please log in to comment.