VDB-354350 · CVE-2026-5213 · GCVE-100-354350

D-LINK DNS-1550-04 UP TO 20260205 /CGI-BIN/ACCOUNT_MGR.CGI CGI_ADDUSER_TO_SESSION READ_LIST STACK-BASED OVERFLOW

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
8.0	$0-$5k	4.10

Summary

A vulnerability labeled as critical has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205. The impacted element is the function `cgi_adduser_to_session` of the file */cgi-bin/account_mgr.cgi*. Such manipulation of the argument *read_list* leads to stack-based overflow. This vulnerability is referenced as CVE-2026-5213. It is possible to launch the attack remotely. Furthermore, an exploit is available.

Details

A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20260205. Affected by this issue is the function `cgi_adduser_to_session` of the file */cgi-bin/account_mgr.cgi*. The manipulation of the argument `read_list` with an unknown input leads to a stack-based overflow vulnerability. Using CWE to declare the problem leads to 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). Impacted is confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is handled as CVE-2026-5213. 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 03/31/2026).

The exploit is available 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.

Similar entries are available at VDB-351120 and VDB-354349.

Product

Vendor

- D-Link

Name

- DNR-202L
- DNR-322L
- DNR-326
- DNS-120
- DNS-315L
- DNS-320
- DNS-320L
- DNS-320LW
- DNS-321
- DNS-323
- DNS-325
- DNS-326
- DNS-327L
- DNS-340L

Version

- 20260205

License

- commercial

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

03/31/2026		Advisory disclosed
03/31/2026	+0 days	VulDB entry created
03/31/2026	+0 days	VulDB entry last update

Sources

Vendor: dlink.com

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5213 (🔒)
GCVE (CVE): GCVE-0-2026-5213

GCVE (VulDB): GCVE-100-354350
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 03/31/2026 12:35 PM
Changes: 03/31/2026 12:35 PM (56)
Complete: 🔍
Submitter: Ziyue Xie
Cache ID: 20:502:179

Submit

Accepted

- Submit #780437: D-Link DNS-120/202L/315L/320/320L/320LW/321/322L/323/325/326/327L/326/340L/343/345/726-4/1100-4/1200-05/1550-04 up to 20260205 Stack-based Buffer Overflow (by Ziyue Xie)

Discussion

No comments yet. Languages: en.

Please log in to comment.