VDB-308050 · CVE-2025-4442 · GCVE-100-308050

D-LINK DIR-605L 2.13B01 FORMSETWAN_WIZARD55 CURTIME BUFFER OVERFLOW

A vulnerability was found in D-Link DIR-605L 2.13B01. It has been declared as critical. This vulnerability affects the function `formSetWAN_Wizard55`. The manipulation of the argument `curTime` with an unknown input leads to a buffer overflow vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability was named CVE-2025-4442. The exploitation appears to be easy. The attack can be initiated remotely. Technical details are known, but there is no available exploit. The structure of the vulnerability defines a possible price range of USD $5k-$25k at the moment (estimation calculated on 05/09/2025).

The vendor was contacted early about this disclosure.

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

Similar entry is available at VDB-240811.

Product

Type

- Router Operating System

Vendor

- D-Link

Name

- DIR-605L

Version

- 2.13B01

License

- commercial

Support

- end of life

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 8.8
VulDB Meta Temp Score: 8.6

VulDB Base Score: 8.8
VulDB Temp Score: 8.5
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 8.8
CNA Vector: 🔒

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

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

Local: No
Remote: Yes

Availability: 🔒
Status: Not defined

EPSS Score: 🔒
EPSS Percentile: 🔒

Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/08/2025		Advisory disclosed
05/08/2025	+0 days	VulDB entry created
05/09/2025	+1 days	VulDB entry last update

Sources

Vendor: dlink.com

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4442 (🔒)
GCVE (CVE): GCVE-0-2025-4442
GCVE (VulDB): GCVE-100-308050
See also: 🔒

Entry

Created: 05/08/2025 07:07 PM
Updated: 05/09/2025 12:45 PM
Changes: 05/08/2025 07:07 PM (55), 05/09/2025 12:45 PM (40)
Complete: 🔍
Submitter: jylsec
Cache ID: 5:749:101

Submit

Accepted

- Submit #558352: D-Link DIR-605L 2.13B01 Buffer Overflow (by jylsec)

Discussion

No comments yet. Languages: en.

Please log in to comment.