



VDB-356329 · CVE-2026-5844 · GCVE-100-356329

D-LINK DIR-882 1.01B02 HNAP1 SETNETWORKSETTINGS PROG.CGI SPRINTF IPADDRESS OS COMMAND INJECTION



CVSS Meta Temp Score

6.5

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

1.24

Summary

A vulnerability, which was classified as **critical**, has been found in **D-Link DIR-882 1.01B02**. The affected element is the function `sprintf` of the file `prog.cgi` of the component *HNAP1 SetNetworkSettings Handler*. This manipulation of the argument `IPAddress` causes os command injection. This vulnerability only affects products that are no longer supported by the maintainer. The identification of this vulnerability is [CVE-2026-5844](#). It is possible to initiate the attack remotely. Furthermore, there is an exploit available.

Details

A vulnerability classified as critical was found in **D-Link DIR-882 1.01B02**. Affected by this vulnerability is the function `sprintf` of the file `prog.cgi` of the component *HNAP1 SetNetworkSettings Handler*. The manipulation of the argument `IPAddress` with an unknown input leads to a os command injection vulnerability. The CWE definition for the vulnerability is [CWE-78](#). The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared at [files.catbox.moe](#). This vulnerability is known as [CVE-2026-5844](#). The exploitation appears to be easy. The attack can be launched remotely. Additional levels of successful authentication are needed for exploitation. Technical details and also a public exploit are known. The price for an exploit might be around USD \$0-\$5k at the moment ([estimation calculated on 04/08/2026](#)). MITRE ATT&CK project uses the attack technique [T1202](#) for this issue.

It is possible to download the exploit at [files.catbox.moe](#). 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 entries [VDB-332400](#), [VDB-332435](#), [VDB-337599](#) and [VDB-337687](#) are related to this item.

Product

Type

- Router Operating System

Vendor

- D-Link

Name

- DIR-882

Version

- 1.01B02

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: 7.2
VulDB Meta Temp Score: 6.5



VulDB Base Score: 7.2
VulDB Temp Score: 6.5
VulDB Vector: 
VulDB Reliability: 

CVSSv2







VulDB Base Score: 
VulDB Temp Score: 
VulDB Reliability: 

Exploiting

Class: Os command injection
CWE: [CWE-78](#) / [CWE-77](#) / [CWE-74](#)
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: files.catbox.moe

Status: Not defined

CVE: [CVE-2026-5844](https://cve.mitre.org/cve/2026/5844) (🗝️)

GCVE (CVE): [GCVE-0-2026-5844](https://www.gdfr.com/gcve/0-2026-5844)

GCVE (VulDB): [GCVE-100-356329](https://www.gdfr.com/gcve/100-356329)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🗝️

Entry

Created: 04/08/2026 08:49 PM

Changes: 04/08/2026 08:49 PM (59)

Complete: 🔍

Submitter: [meshaal](#)

Cache ID: 4:1E3:179

Submit

Accepted

- [Submit #790290: D-Link DIR-882 1.01B02 OS Command Injection \(by meshaal\)](#)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)