



D-Link DIR-823X set_wifidog_settings sub_412E7C command injection

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary

CVE	CVE-2026-1125
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-18 16:15:50 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A weakness has been identified in D-Link DIR-823X 250416. Affected by this issue is the function sub_412E7C of the file /c

Risk And Classification

Primary CVSS: v4.0 5.5 MEDIUM from cna@vulldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-74 | CWE-77 | CWE-77 Command Injection | CWE-74 Injection

Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	5.5	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C
4.0	CNA	DECLARED	6.9	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	cna@vulldb.com	Secondary	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	7.3	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
3.0	CNA	DECLARED	7.3	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R
2.0	cna@vulldb.com	Secondary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X



CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

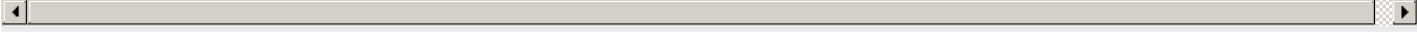
Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

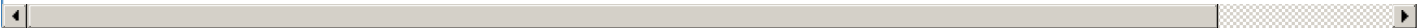
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:X/RC:R



NVD Known Affected Configurations (CPE 2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dir-823x	-	All	All	All
Operating System	Dlink	Dir-823x Firmware	250126	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	D-Link	DIR-823X	affected 250416	Not specified

References				
Reference	Source	Link	Tags	
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advis	
www.dlink.com	cna@vuldb.com	www.dlink.com	Product	
vuldb.com	cna@vuldb.com	vuldb.com	Third Party Advis	
vuldb.com	cna@vuldb.com	vuldb.com		
vuldb.com	cna@vuldb.com	vuldb.com	Permissions Req	
github.com/DavCloudz/cve/blob/main/D-link/DIR_823X/DIR-823X%20V250416%20...	cna@vuldb.com	github.com	Exploit, Third Par	
CVE Program record	CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analys	



Vendor Comments And Credit	
Discovery Credit	

Additional Advisory Data

Source	Time	Event
CNA	2026-01-17T00:00:00.000Z	Advisory disclosed
CNA	2026-01-17T01:00:00.000Z	VulDB entry created
CNA	2026-01-31T02:47:43.000Z	VulDB entry last update

There are currently no legacy QID mappings associated with this CVE.