D-Link DIR-825 miniupnpd upnpsoap.c AddPortMapping buffer overflow

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-7069
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-27 00:16:21 UTC
Updated	2026-04-27 00:16:21 UTC
Description	A security flaw has been discovered in D-Link DIR-825 up to 3.00b32. This impacts the function AddPortMapping of the file

Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from cna@vuldb.com

CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-119 | CWE-120 | CWE-120 Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	8.6	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	8.6	HIGH	CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	8	HIGH	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8	HIGH	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R
3.0	CNA	DECLARED	8	HIGH	CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R
2.0	cna@vuldb.com	Secondary	7.7		AV:A/AC:L/Au:S/C:C/I:C/A:C
2.0	CNA	DECLARED	7.7		AV:A/AC:L/Au:S/C:C/I:C/A:C/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:A/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	D-Link	DIR-825	affected 3.00b32	Not specified

References

Reference	Source	Link	Tags
vuldb.com/vuln/359644	cna@vuldb.com	vuldb.com	
vuldb.com/submit/798647	cna@vuldb.com	vuldb.com	
www.dlink.com	cna@vuldb.com	www.dlink.com	
vuldb.com/vuln/359644/cti	cna@vuldb.com	vuldb.com	
tzh00203.notion.site/D-Link-DIR-825-miniupnpd-AddPortMapping-Stack-Overflow-337b5c...	cna@vuldb.com	tzh00203.notion.site	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

Vendor Comments And Credit

Discovery Credit

CNA: tian (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-26T00:00:00.000Z	Advisory disclosed
CNA	2026-04-26T02:00:00.000Z	VulDB entry created

CNA	2026-04-26T09:43:11.000Z	VulDB entry last update

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