D-Link DNS-1550-04 account_mgr.cgi cgi_addgroup_get_group_quota_minsize stack-based overflow

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-5214
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-31 22:16:22 UTC
Updated	2026-04-02 17:16:00 UTC
Description	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-3

Risk And Classification

Primary CVSS: v4.0 7.4 HIGH from cna@vuldb.com

CVSS:4.0/AV:N/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

EPSS: 0.000450000 probability, percentile 0.136560000 (date 2026-04-01)

Problem Types: CWE-119 | CWE-121 | CWE-787 | CWE-121 Stack-based Buffer Overflow | CWE-119 Memory Corruption

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	7.4	HIGH	CVSS:4.0/AV:N/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	8.7	HIGH	CVSS:4.0/AV:N/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	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R
3.0	CNA	DECLARED	8.8	HIGH	CVSS:3.0/AV:N/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	9		AV:N/AC:L/Au:S/C:C/I:C/A:C
2.0	CNA	DECLARED	9		AV:N/AC:L/Au:S/C:C/I:C/A:C/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

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:N/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

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Dlink	Dnr-202l	-	All	All	All
Operating System	Dlink	Dnr-202l Firmware	All	All	All	All
Hardware	Dlink	Dnr-326	-	All	All	All
Operating System	Dlink	Dnr-326 Firmware	All	All	All	All
Hardware	Dlink	Dns-1100-4	-	All	All	All
Operating System	Dlink	Dns-1100-4 Firmware	All	All	All	All
Hardware	Dlink	Dns-120	-	All	All	All
Hardware	Dlink	Dns-1200-05	-	All	All	All
Operating System	Dlink	Dns-1200-05 Firmware	All	All	All	All
Operating System	Dlink	Dns-120 Firmware	All	All	All	All
Hardware	Dlink	Dns-1550-04	-	All	All	All
Operating System	Dlink	Dns-1550-04 Firmware	All	All	All	All
Hardware	Dlink	Dns-315l	-	All	All	All
Operating System	Dlink	Dns-315l Firmware	All	All	All	All
Hardware	Dlink	Dns-320	-	All	All	All
Hardware	Dlink	Dns-320l	-	All	All	All
Hardware	Dlink	Dns-320lw	-	All	All	All
Operating System	Dlink	Dns-320lw Firmware	All	All	All	All

Operating System	Dlink	Dns-320l Firmware	All	All	All	All
Operating System	Dlink	Dns-320 Firmware	All	All	All	All
Hardware	Dlink	Dns-321	-	All	All	All
Operating System	Dlink	Dns-321 Firmware	All	All	All	All
Hardware	Dlink	Dns-322l	-	All	All	All
Operating System	Dlink	Dns-322l Firmware	All	All	All	All
Hardware	Dlink	Dns-323	-	All	All	All
Operating System	Dlink	Dns-323 Firmware	All	All	All	All
Hardware	Dlink	Dns-325	-	All	All	All
Operating System	Dlink	Dns-325 Firmware	All	All	All	All
Hardware	Dlink	Dns-326	-	All	All	All
Operating System	Dlink	Dns-326 Firmware	All	All	All	All
Hardware	Dlink	Dns-327l	-	All	All	All
Operating System	Dlink	Dns-327l Firmware	All	All	All	All
Hardware	Dlink	Dns-340l	-	All	All	All
Operating System	Dlink	Dns-340l Firmware	All	All	All	All
Hardware	Dlink	Dns-343	-	All	All	All
Operating System	Dlink	Dns-343 Firmware	All	All	All	All
Hardware	Dlink	Dns-345	-	All	All	All
Operating System	Dlink	Dns-345 Firmware	All	All	All	All
Hardware	Dlink	Dns-726-4	-	All	All	All
Operating System	Dlink	Dns-726-4 Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	D-Link	DNS-120	affected 20260205	Not specified
CNA	D-Link	DNR-202L	affected 20260205	Not specified
CNA	D-Link	DNS-315L	affected 20260205	Not specified
CNA	D-Link	DNS-320	affected 20260205	Not specified
CNA	D-Link	DNS-320L	affected 20260205	Not specified
CNA	D-Link	DNS-320LW	affected 20260205	Not specified
CNA	D-Link	DNS-321	affected 20260205	Not specified
CNA	D-Link	DNR-322L	affected 20260205	Not specified
CNA	D-Link	DNS-323	affected 20260205	Not specified
CNA	D-Link	DNS-325	affected 20260205	Not specified

CNA	D-Link	DNS-326	affected 20260205	Not specified
CNA	D-Link	DNS-327L	affected 20260205	Not specified
CNA	D-Link	DNR-326	affected 20260205	Not specified
CNA	D-Link	DNS-340L	affected 20260205	Not specified
CNA	D-Link	DNS-343	affected 20260205	Not specified
CNA	D-Link	DNS-345	affected 20260205	Not specified
CNA	D-Link	DNS-726-4	affected 20260205	Not specified
CNA	D-Link	DNS-1100-4	affected 20260205	Not specified
CNA	D-Link	DNS-1200-05	affected 20260205	Not specified
CNA	D-Link	DNS-1550-04	affected 20260205	Not specified

References

Reference	Source	Link	Tags
vuldb.com/vuln/354349	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry
vuldb.com/submit/780439	cna@vuldb.com	vuldb.com	Third Party Advisory, VDB Entry
www.dlink.com	cna@vuldb.com	www.dlink.com	Product
github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_169/169.md	cna@vuldb.com	github.com	Exploit, Third Party Advisory
vuldb.com/vuln/354349/cti	cna@vuldb.com	vuldb.com	Permissions Required, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Ziyue Xie (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-31T00:00:00.000Z	Advisory disclosed
CNA	2026-03-31T02:00:00.000Z	VulDB entry created
CNA	2026-03-31T12:35:06.000Z	VulDB entry last update

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report