



# D-Link DNS-1550-04 account\_mgr.cgi cgi\_adduser\_to\_session stack-based overflow

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-5213
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulDB
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-31 21:16:34 UTC
<b>Updated</b>	2026-04-02 17:15:28 UTC
<b>Description</b>	A vulnerability was determined in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, D

## 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/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000450000 probability, percentile 0.137530000 (date 2026-04-02)

**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/MSX/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	<a href="#">Dlink</a>	<a href="#">Dns-320 Firmware</a>	All	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-320 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-321</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-321 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-322l</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-322l Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-323</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-323 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-325</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-325 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-326</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-326 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-327l</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-327l Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-340l</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-340l Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-343</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-343 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-345</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-345 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dns-726-4</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dns-726-4 Firmware</a>	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">D-Link</a>	<a href="#">DNS-120</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNR-202L</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-315L</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-320</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-320L</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-320LW</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-321</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNR-322L</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-323</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-325</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-326</a>	affected 20260205	Not specified

CNA	<a href="#">D-Link</a>	<a href="#">DNS-327L</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNR-326</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-340L</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-343</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-345</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-726-4</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-1100-4</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-1200-05</a>	affected 20260205	Not specified
CNA	<a href="#">D-Link</a>	<a href="#">DNS-1550-04</a>	affected 20260205	Not specified

## References

Reference	Source	Link	Tags
<a href="https://vuldb.com/vuln/354350/cti">vuldb.com/vuln/354350/cti</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://vuldb.com">vuldb.com</a>	Permissions Required, VDB Entry
<a href="https://vuldb.com/vuln/354350">vuldb.com/vuln/354350</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://vuldb.com">vuldb.com</a>	Third Party Advisory, VDB Entry
<a href="https://www.dlink.com">www.dlink.com</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://www.dlink.com">www.dlink.com</a>	Product
<a href="https://github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_168/168.md">github.com/wudipjq/my_vuln/blob/main/D-Link8/vuln_168/168.md</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://github.com">github.com</a>	Exploit, Third Party Advisory
<a href="https://vuldb.com/submit/780437">vuldb.com/submit/780437</a>	<a href="mailto:cna@vuldb.com">cna@vuldb.com</a>	<a href="https://vuldb.com">vuldb.com</a>	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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	2026-03-31T12:35:09.000Z	VulDB entry last update

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

CVE, CWE, and OVAL are registered 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](#)**