LB-LINK BL-AC3600 shadow hard-coded credentials

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

Summary

CVE	CVE-2025-7564
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-07-14 03:15:24 UTC
Updated	2026-04-29 01:00:01 UTC
Description	A vulnerability, which was classified as critical, has been found in LB-LINK BL-AC3600 1.0.22. Affected by this issue is som

Risk And Classification

Primary CVSS: v4.0 7.1 HIGH from cna@vuldb.com

CVSS:4.0/AV:L/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-259 | CWE-798 | CWE-798 Hard-coded Credentials | CWE-259 Use of Hard-coded Password

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	7.1	HIGH	CVSS:4.0/AV:L/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	8.5	HIGH	CVSS:4.0/AV:L/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	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R
3.0	CNA	DECLARED	7.8	HIGH	CVSS:3.0/AV:L/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	6.8		AV:L/AC:L/Au:S/C:C/I:C/A:C
2.0	CNA	DECLARED	6.8		AV:L/AC:L/Au:S/C:C/I:C/A:C/E:POC/RL:ND/RC:UR

CVSS v4.0 Breakdown

Attack Vector

Local

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:L/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

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:L/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	Lb-link	Bl-ac3600	-	All	All	All
Operating System	Lb-link	Bl-ac3600 Firmware	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	LB-LINK	BL-AC3600	affected 1.0.22	Not specified

References

Reference	Source	Link
github.com/waiwai24/0101/blob/main/CVEs/Blink/Hardcoded_Credentials_in_B...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
vuldb.com	cna@vuldb.com	vuldb.com
vuldb.com	cna@vuldb.com	vuldb.com
github.com/waiwai24/0101/blob/main/CVEs/Blink/Hardcoded_Credentials_in_B...	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
vuldb.com	cna@vuldb.com	vuldb.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: waiwai24 (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-07-12T00:00:00.000Z	Advisory disclosed
CNA	2025-07-12T02:00:00.000Z	VulDB entry created
CNA	2025-07-12T23:17:06.000Z	VulDB entry last update

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