



CVE-2023-27748

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-27748
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-13 20:15:00 UTC
Updated	2023-04-25 13:38:00 UTC
Description	BlackVue DR750-2CH LTE v.1.012_2022.10.26 does not employ authenticity check for uploaded firmware. This can allow a

Risk And Classification

Problem Types: CWE-345

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Blackvue	Dr750-2ch Ir Lte	-	All	All	All
Operating System	Blackvue	Dr750-2ch Ir Lte Firmware	1.012_2022.10.26	All	All	All
Hardware	Blackvue	Dr750-2ch Lte	-	All	All	All
Operating System	Blackvue	Dr750-2ch Lte Firmware	1.012_2022.10.26	All	All	All

References

Reference	Source	Link
GitHub - eyJhb/BlackVue CVE CVE-2023-27746 CVE-2023-27747 CVE-2023-27748	MISC	github.com
GitHub - eyJhb/BlackVue CVE CVE-2023-27746 CVE-2023-27747 CVE-2023-27748	MISC	github.com
Home - BlackVue Dash Cameras	MISC	blackvue.com
DR750-2CH IR LTE - BlackVue Online Store	MISC	shop.blackvue.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)