



# CVE-2022-2472

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

## Summary

<b>CVE</b>	CVE-2022-2472
<b>State</b>	PUBLIC
<b>Assigner</b>	cve-requests@bitdefender.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-15 14:15:00 UTC
<b>Updated</b>	2022-09-19 19:03:00 UTC
<b>Description</b>	Improper Initialization vulnerability in the local server component of EZVIZ CS-C6N-A0-1C2WFR allows a local attacker to r

## Risk And Classification

**Problem Types:** CWE-665

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Ezviz	Cs-c6n-a0-1c2wfr	-	All	All	All
Operating System	Ezviz	Cs-c6n-a0-1c2wfr Firmware	5.3.0	build220428	All	All

## References

Reference	Source	Link	Tags
Vulnerabilities Identified in EZVIZ Smart Cams	MISC	<a href="http://www.bitdefender.com">www.bitdefender.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Bitdefender Labs

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

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)