



# CVE-2023-41613

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

## Summary

<b>CVE</b>	CVE-2023-41613
<b>State</b>	RESERVED
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-12-04 14:15:00 UTC
<b>Updated</b>	2023-12-07 21:08:00 UTC
<b>Description</b>	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new

## Risk And Classification

**Problem Types:** CWE-427

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Ezviz</a>	<a href="#">Ezviz Studio</a>	2.2.0	All	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows</a>	-	All	All	All

## References

Reference	Source	Link	Tags
EzViz Studio 2.2.0 DLL Hijacking ≈ Packet Storm		<a href="#">packetstormsecurity.com</a>	Exploit, Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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](#).

**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)