



# CVE-2023-38949

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

## Summary

<b>CVE</b>	CVE-2023-38949
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-08-03 23:15:00 UTC
<b>Updated</b>	2023-08-08 19:02:00 UTC
<b>Description</b>	An issue in a hidden API in ZKTeco BioTime v8.5.5 allows unauthenticated attackers to arbitrarily reset the Administrator password.

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zkteco	Biotime	8.5.5	All	All	All

## References

Reference	Source	Link	Tags
CVE-2023-38949   Claroty	MISC	<a href="https://claroty.com">claroty.com</a>	
ZKTeco   Home Page	MISC	<a href="https://zkteco.com">zkteco.com</a>	
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

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)