

CVE-2023-38950

ZKTeco BioTime Path Traversal Vulnerability

CISA KEV since May 19, 2025

Actively exploited

A path traversal vulnerability in the iclock API of ZKTeco BioTime v8.5.5 allows unauthenticated attackers to read arbitrary files via supplying a crafted payload. This vulnerability was fixed in version 9.0.120240617.19506 of ZKBioTime.

EVRS 83 / ₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.925 99.83rd percentile · FIRST	CISA DEADLINE Jun 9, 2025 KEV since 2025 · listed over a year
---	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.925 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
biotime	< 9.0.1	9.0.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-27mv-5vpc-8g53
NVD nvd.nist.gov/vuln/detail/CVE-2023-38950
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-42710

zkteco.com zkteco.com/en/Security_Bulletinsibs
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2023-38950

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.