ZKTeco Biometric System Found Vulnerable to 24 Critical Security Flaws

Date: 15th June 2024 | Severity: High

Summary

ZKTeco has uncovered 24 security flaws that could be used by attackers to defeat authentication, steal biometric data, and even deploy malicious backdoors. the newly discovered vulnerabilities expose them to various attacks. Kaspersky grouped the flaws based on the required patches and registered them under specific CVEs (Common Vulnerabilities and Exposures).

Attack Vectors

- By adding random user data to the database or using a fake QR code, a nefarious actor can easily bypass the verification process and gain unauthorized access," Kaspersky said. "Attackers can also steal and leak biometric data, remotely manipulate devices, and deploy backdoors.
- The 24 flaws span six SQL injections, seven stack-based buffer overflows, five command injections, four arbitrary file writes, and two arbitrary file reads.
- Bypassing Verification: Attackers can exploit the system by adding random user data to the database or using a fake QR code. This allows them to bypass the verification process and gain unauthorized access.
- Biometric Data Theft: The vulnerabilities enable theft and potential leakage of biometric data from the compromised system.
- Remote Manipulation: Malicious actors can remotely manipulate the devices, compromising their functionality.
- Backdoor Deployment: Certain flaws allow attackers to deploy backdoors, granting unauthorized network access.

Indicator of compromise

INDICATOR TYPE	INDICATORS
CVE	• CVE-2023-3938, allows cybercriminals to perform a SQL injection, which involves inserting malicious code into strings sent to a terminal's database. • CVE-2023-3939 (CVSS score: 10.0) - A set of command injection flaws that allows for execution of arbitrary OS commands with root privileges. • CVE-2023-3940 involves flaws in a software component that permits arbitrary file reading. • CVE-2023-3941, threat actors can upload their own data, such as photos, thereby adding unauthorized individuals to the database. • CVE-2023-3942 provides another way to retrieve sensitive user and system information from the biometry devices' databases – through SQL injection attacks. • CVE-2023-3943 - A set of stack-based buffer overflow flaws that allows an attacker to execute arbitrary code

Recommendation

- Isolate biometric reader usage into a separate network segment.
- Employ robust administrator passwords, changing default ones.
- Audit and bolster device's security settings, fortifying weak defaults.
- Consider enabling or adding temperature detection to avoid authorization using a random photo.
- Minimize the use of QR-code functionality, if feasible.
- Update firmware regularly.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https[:]//thehackernews.com/2024/06/zkteco-biometric-system-found.html
- https[:]//www.kaspersky.com/about/press-releases/2024_kaspersky-finds-24-vulnerabilities-in-chinese-biometric-access-systems
- https[:]//www.infosecurity-magazine.com/news/kaspersky-flaws-chinese-biometric/