مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in SICK DL100 Devices

Tracking #:432316996

Date:21-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Multiple critical vulnerabilities have been discovered in SICK DL100-2xxxxxxx device exposing them to potential code execution and password-related attacks.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been discovered in SICK DL100-2xxxxxxx devices, exposing them to potential code execution and password-related attacks. The vulnerabilities, identified as CVE-2025-27593, CVE-2025-27594, and CVE-2025-27595, affect all firmware versions of the SICK DL100-2xxxxxxx products. These flaws could allow attackers to distribute malicious code, intercept authentication data, and easily calculate matching passwords, compromising the security and integrity of the affected devices.

Key Vulnerabilities:

- CVE-2025-27593: Download of Code Without Integrity Check (CVSS v3.1 Base Score: 9.3)
- CVE-2025-27594: Cleartext Transmission of Sensitive Information (CVSS v3.1 Base Score: 7.5)
- CVE-2025-27595: Use of Weak Hash (CVSS v3.1 Base Score: 9.8)

Mitigation Strategies:

- Network Isolation: Minimize network exposure of the affected devices and restrict network access to trusted entities only.
- Secure Infrastructure: Operate the affected systems within a protected IT environment, following recommended security practices.
- Monitoring and Auditing: Implement robust logging and monitoring solutions to detect and respond to suspicious activities promptly.
- Firmware Updates: Stay informed about upcoming firmware updates from SICK and apply them as soon as they become available.
- Strong Authentication: Implement multi-factor authentication where possible and ensure all default credentials are changed.

RECOMMENDATIONS:

- Implement network segmentation to isolate affected devices.
- Apply vendor-provided workarounds for each CVE.
- Regularly monitor and audit device access and activities.
- Update firmware as soon as patches become available.
- Implement strong authentication mechanisms and change default credentials.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.sick.com/.well-known/csaf/white/2025/sca-2025-0004.pdf