مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Critical Vulnerability in SICK Products

Tracking #:432316438

Date:25-10-2024



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council observed a critical vulnerability identified as CVE-2024-10025 has been discovered in certain SICK products.

## TECHNICAL DETAILS:

A critical vulnerability identified as CVE-2024-10025 has been discovered in certain SICK products. This vulnerability stems from the use of hard-coded credentials stored in plain text within the .sdd file, which can be exploited by attackers to gain unauthorized access as an "Authorized Client" if default passwords are not changed. The vulnerability has a CVSS v3.1 base score of 9.1, indicating its critical severity.

**Affected Products:**

- SICK CLV6xx: All versions
- SICK Lector6xx: All versions
- SICK RFx6xx: All versions

**Remediations:**

- Change all default passwords on affected SICK products to prevent unauthorized access.

## RECOMMENDATIONS:

1. **Immediate Action**: Change all default passwords on affected SICK products to prevent unauthorized access.
2. **Implement Strong Password Policies**: Ensure robust credentials are used across all systems.
3. **Regular Audits**: Conduct regular audits and updates of passwords to maintain security integrity.
4. **Network Segmentation**: If possible, implement network segmentation to limit access to affected devices.
5. **Monitoring**: Continuously monitor for unauthorized access attempts or suspicious activities on these products.
6. **Stay Informed**: Keep abreast of any patches or updates released by SICK for this vulnerability and apply them promptly.

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/2024/sca-2024-0003.pdf