مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Daikin Security Gateway

Tracking #:432317716

Date:16-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Daikin Security Gateway systems that could allow attackers to bypass authentication and gain unauthorized access to industrial control systems.

TECHNICAL DETAILS:

A critical authentication bypass vulnerability exists in Daikin Security Gateway systems used widely in industrial control and energy sector environments. This vulnerability allows unauthenticated attackers to completely bypass login mechanisms via manipulation of a weak password recovery feature. Exploitation requires no privileges or user interaction and remote attack is possible over the network. Public proof-of-concept exploits exist, posing a severe threat to affected organizations.

Vulnerability Details

- CVE-2025-10127
- CVSS v3.1 Score 9.8 (Critical)
- Vulnerability Type: Weak Password Recovery Mechanism (CWE-640)
- The vulnerability resides in the Security Gateway's password recovery functionality, where an attacker can use a crafted user-controlled key to bypass authentication mechanisms entirely. This flaw enables unrestricted access to gateway systems managing industrial control operations, allowing attackers to access or modify sensitive ICS data and disrupt critical infrastructure operations without any prior credentials.
- Successful exploitation could result in:
  - Unauthorized access to sensitive industrial control data
  - Modification of system configurations
  - Disruption of critical energy sector operations
  - Complete compromise of system confidentiality, integrity, and availability
- Exploit Availability: Public Proof of Concept (PoC) available

Affected Products:

- Daikin Security Gateway: App: 100, Frm: 214

RECOMMENDATIONS:

Since vendor patches are not available, organizations must implement strong defense-in-depth controls to mitigate exploitation:

- Restrict Exposure: Place Daikin Security Gateway systems behind firewalls and ensure they cannot be accessed over the public internet.
- Segmentation: Isolate ICS networks from corporate IT networks and untrusted environments.
- Remote Access Protections: If remote access is required, use secure VPN solutions and enforce strict device authentication.
- Network Hardening: Limit network exposure of control system devices; allow access only from trusted management networks.
- Monitoring & Detection: Continuously monitor for anomalous access attempts against Daikin Security Gateway systems.
- Incident Response Preparedness: Review contingency and recovery plans in case of system compromise or operational disruption.

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://nvd.nist.gov/vuln/detail/CVE-2025-10127