مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical RCE Vulnerability in HIKVISION applyCT

Tracking #:432317456

Date:07-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical unauthenticated remote code execution (RCE) vulnerability, tracked as CVE-2025-34067, has been identified in HIKVISION's applyCT platform, also known as HikCentral.

TECHNICAL DETAILS:

A critical unauthenticated remote code execution (RCE) vulnerability, tracked as CVE-2025-34067, has been identified in HIKVISION's applyCT platform, also known as HikCentral. This vulnerability affects a key endpoint (/bic/ssoService/v1/applyCT) and stems from the use of a vulnerable version of the Fastjson library. Exploitation allows remote attackers to execute arbitrary code without authentication, potentially leading to full system compromise, data theft, surveillance manipulation, and broader lateral movement within the network.

This platform is widely deployed in government, industrial, and commercial surveillance systems, making this vulnerability a high-value target for threat actors. Immediate action is strongly recommended.

Vulnerability Details:

- CVE ID: CVE-2025-34067
- CVSS-B 10.0 CRITICAL
- Affected Product: applyCT (HikCentral)
- Vulnerability Type: Unauthenticated Remote Code Execution (RCE)
- Attack Vector: Network (No authentication required)
- Exploit Mechanism:
  - Malicious JSON payloads are sent to the vulnerable endpoint
  - Payload references Java class JdbcRowSetImpl and an attacker-controlled LDAP server
  - Leads to execution of arbitrary Java code on the server
- Proof-of-Concept (PoC):
  - POST request with specially crafted JSON using LDAP reference
  - Remote class loading leads to code execution

Potential Impact

- Full compromise of affected server
- Unauthorized access to sensitive surveillance and management data
- Disruption or manipulation of security camera feeds
- Lateral movement within enterprise networks
- Potential for ransomware deployment
- Financial loss, reputational damage, and regulatory penalties

RECOMMENDATIONS:

- Update HikCentral to the latest version that removes or secures the use of vulnerable Fastjson.
- Apply all official security patches released by HIKVISION as soon as possible.

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-2025-34067