مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Hikvision HikCentral Professional Software

Tracking #:432315682
Date:07-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple Vulnerabilities in Hikvision HikCentral Professional software that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

1.CVE-2024-25063

- CVSS v3.1 score: 7.5 HIGH
- Insufficient server-side validation could allow attackers to gain unauthorized access to certain URLs within the system.

2.CVE-2024-25064:

- CVSS v3.1 score: 4.3
- Insufficient server-side validation could allow an attacker with login privileges to access unauthorized resources by modifying parameter values.

Affected Products:

- HikCentral Professional versions below V2.5.1 (including V2.5.1) are affected by CVE-2024-25063.
- HikCentral Professional versions after V2.0.0 and before V2.5.1 are affected by CVE-2024-25064.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Hikvision.

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.hikvision.com/en/support/cybersecurity/security-advisory/security-vulnerabilities-in-hikcentral-professional/