مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Remote Command Execution Vulnerability in Hikvision Wireless Access Points

Tracking #:432317382
Date:16-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Hikvision Wireless Access Points that could be exploited to execute malicious commands on affected devices.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-39240**
- CVSS v3.1 score: 7.2 High
- A security vulnerability exists in some Hikvision Wireless Access Point (WAP) models. The flaw arises from insufficient input validation, which allows authenticated attackers to execute arbitrary system commands by sending specially crafted packets to the vulnerable devices.
- Successful exploitation of this vulnerability requires valid credentials and can lead to remote code execution, compromising confidentiality, integrity, and availability of the device.

Affected Products and Fixed Versions:

Product Model	Affected Version	Fixed Version
DS-3WAP622G-SI	V1.1.5402 build241014 (E2254P02) and the versions prior to it	V1.1.6300 build250331 (R2263)
DS-3WAP623E-SI	V1.1.5400 build240814 (E2254) and the versions prior to it	V1.1.6300 build250331 (R2263)
DS-3WAP521-SI	V1.1.5400 build240814 (E2254) and the versions prior to it	V1.1.6300 build250331 (R2263)
DS-3WAP522-SI	V1.1.5402 build241014 (E2254P02) and the versions prior to it	V1.1.6300 build250331 (R2263)
DS-3WAP621E-SI	V1.1.5400 build240814 (E2254) and the versions prior to it	V1.1.6300 build250331 (R2263)
DS-3WAP622E-SI	V1.1.5402 build241014 (E2254P02) and the versions prior to it	V1.1.6300 build250331 (R2263)

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/remote-command-execution-vulnerability-in-some-hikvision-wireless-access-point/