مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Remote Code Execution Vulnerability in Synology Camera

Tracking #:432316993

Date:20-03-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical security vulnerability (CVE-2024-11131) has been identified in Synology Camera Firmware affecting BC500, CC400W, and TC500 models.

TECHNICAL DETAILS:

A critical security vulnerability (CVE-2024-11131) has been identified in Synology Camera Firmware affecting BC500, CC400W, and TC500 models.

Vulnerability Details

- **CVE Identifier**: CVE-2024-11131
- **Severity**: Critical
- **CVSS3 Base Score**: 9.8
- **CVSS3 Vector**: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **Vulnerability Type**: Out-of-Bounds Read
- **Impact**: Remote Code Execution
- **Attack Vector**: Remote, Network-based
- This vulnerability exists due to an out-of-bounds read within the video interface, allowing unauthenticated remote attackers to execute arbitrary code on the affected devices via unspecified vectors. Exploiting this flaw could result in full system compromise, unauthorized access, and potential network infiltration.
- **Affected Models**: BC500, CC400W, and TC500 models.
- **Fixed Version**: 1.2.0-0525 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update all affected devices firmware version to the fixed version.

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.synology.com/en-global/security/advisory/Synology_SA_24_24