مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Synology Media Server

Tracking #:432316907

Date: 26-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Synology has identified and patched a security issue in its Media Server software that could allow unauthorized access to files on affected devices.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-4464**
- CVSS3 Base Score: 7.5 High
- A security vulnerability exists in Synology Media Server that allows unauthenticated remote attackers to read specific files on the Synology device. This vulnerability stems from an authorization bypass related to user-controlled keys within the streaming service.
- An authorization bypass through a user-controlled key vulnerability in the streaming service of Synology Media Server before 1.4-2680, 2.0.5-3152, and 2.2.0-3325 allows remote attackers to read specific files via unspecified vectors.
- Successful exploitation of this vulnerability could allow an unauthorized remote attacker to read sensitive files on the Synology device. This could lead to information disclosure and potential further compromise.

Fixed Versions:

- Media Server for DSM 7.2- Upgrade to 2.2.0-3325 or above.
- Media Server for DSM 7.1- Upgrade to 2.0.5-3152 or above.
- Media Server for SRM 1.3- Upgrade to 1.4-2680 or above.

RECOMMENDATIONS:

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

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-my/security/advisory/Synology_SA_24_28