مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Synology DSM

Tracking #:432318043

Date:20-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Synology DSM that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2025-13392
- CVSS3 Base Score: 8.1 High
- A high-severity authentication bypass vulnerability exists in affected DSM versions. Successful exploitation allows a remote attacker to bypass authentication mechanisms if they possess prior knowledge of a valid distinguished name (DN). This may lead to unauthorized access and compromise of system security.
- **Impact:** Allows remote attackers to bypass authentication using known DN information.

Affected Products and Fixed Versions

- **DSM 7.3:** Upgrade to version **7.3.1-86003-1** or later.
- **DSM 7.2.2:** Upgrade to version **7.2.2-72806-5** or later.

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_25_14