مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Apache Syncope AES Default Encryption Key Vulnerability

Tracking #:432318067

Date:25-11-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability has been disclosed in Apache Syncope, impacting versions that support AES encryption for storing internal user password values.

TECHNICAL DETAILS:

A security vulnerability (CVE-2025-65998) has been disclosed in Apache Syncope, impacting versions that support AES encryption for storing internal user password values. When AES is enabled, Syncope uses a hard-coded, default AES encryption key, making it possible for attackers who gain access to the database to decrypt and recover cleartext passwords.

The severity is rated Important due to the risk of credential disclosure and potential privilege escalation across connected systems. Users and administrators should immediately upgrade to Syncope 3.0.15 or 4.0.3, which introduce proper key management and remove the insecure default.

Vulnerability Details:

- CVE-2025-65998
- Base Score: 7.5 (High)
- Description: Apache Syncope allows optional configuration to store user passwords using AES encryption within its internal database. However:

    - When AES encryption is enabled,
    - The application uses a hard-coded default AES key embedded in the source code,
    - Instead of generating or requiring a unique, deployment-specific key.

  This design flaw enables any attacker who gains access to Syncope's internal database to:

    1. Retrieve the AES-encrypted password values.
    2. Use the known hard-coded key to decrypt every stored password.
    3. Recover the original cleartext credentials.

  These credentials may grant access not only to Syncope itself but also to downstream systems integrated via provisioning connectors

- Affected Versions:
    - Versions 2.1 – 2.1.14
    - Versions 3.0 – 3.0.14
    - Versions 4.0 – 4.0.2

- Fixed Versions:
    - 3.0.15
    - 4.0.3

RECOMMENDATIONS:

- Immediate upgrade Apache Syncope to one of the fixed versions

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://lists.apache.org/thread/fjh0tb0d1xkbphc5ogdsc348ppz88cts