مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Account Takeover Vulnerability in ADSelfService Plus

Tracking #:432316927

Date:04-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability has been identified in ManageEngine ADSelfService Plus, a widely used self-service password management and single sign-on solution.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2025-1723) has been identified in ManageEngine ADSelfService Plus, a widely used self-service password management and single sign-on solution.

Vulnerability Details:

- **CVE ID: CVE-2025-1723**
- **Severity: High**
- The vulnerability arises due to improper session handling in ADSelfService Plus, which could allow unauthorized access to user enrollment data when multi-factor authentication (MFA) is not enabled for the ADSelfService Plus login. This could enable attackers to access sensitive information and potentially compromise user accounts.

Affected Versions:

- ADSelfService Plus builds 6510 and earlier

Fixed Version:

- ADSelfService Plus builds 6511

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade ADSelfService Plus to the fixed version or latest version to patch the vulnerability.

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.manageengine.com/products/self-service-password/advisory/CVE-2025-1723.html