مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Account Takeover Vulnerability in ManageEngine Products

Tracking #:432319149

Date:17-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability, CVE-2026-11374, has been identified in ManageEngine products when deployed as integrated components within ManageEngine AD360.

TECHNICAL DETAILS:

A high-severity vulnerability, CVE-2026-11374, has been identified in ManageEngine ADSelfService Plus, ManageEngine RecoveryManager Plus, ManageEngine M365 Manager Plus, and ManageEngine ADAudit Plus when deployed as integrated components within ManageEngine AD360. The vulnerability stems from predictable Single Sign-On (SSO) ticket generation. An unauthenticated attacker may be able to predict valid SSO authentication tickets, obtain user identity and role information, and ultimately take over targeted user accounts.

Vulnerability Details:

- CVE ID: CVE-2026-11374
- Severity: High
- Vulnerability Type: Predictable Authentication Token / Account Takeover
- Authentication Required: No
- Attack Vector: Network
- Affected Environment: Products integrated with ManageEngine AD360 using SSO

Affected products and fixed version:

Product	Affected Versions	Fixed Version
ADSelfService Plus	6528 and earlier	6529
RecoveryManager Plus	6320 and earlier	6321
M365 Manager Plus	4816 and earlier	4817
ADAudit Plus	8702 and earlier	8703

RECOMMENDATIONS:

- Organizations using affected products integrated with AD360 should immediately upgrade to the patched versions released by the vendor.

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-2026-11374.html