مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - ManageEngine Analytics Plus

Tracking #:432316981

Date:18-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high-severity has been identified in ManageEngine Analytics Plus on-premise allows attackers to compromise Active Directory (AD)-authenticated user accounts.

TECHNICAL DETAILS:

A high-severity authentication bypass vulnerability (CVE-2025-1724, CVSS 7.4) in ManageEngine Analytics Plus on-premise allows attackers to compromise Active Directory (AD)-authenticated user accounts.

Vulnerability Details

- CVE ID: CVE-2025-1724
- Severity: High
- Product Affected: Analytics Plus on-premise (Windows)
- Impacted Versions: All Windows builds below 6130
- Fixed Version: Build 6130
- Impact: Unauthorized access to authenticated AD user accounts, potentially leading to account takeovers and data breaches.
- Applicability: Affects Windows installations using Active Directory authentication without Active Directory SSO configuration.

RECOMMENDATIONS:

- Ensure all Analytics Plus on-premise instances are updated promptly with the latest security patches.
- Enable Active Directory SSO configuration and Enforce multi-factor authentication (MFA) for AD users.

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/analytics-plus/CVE-2025-1724.html