



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-severity Vulnerability in Analytics Plus

Tracking #:432316573

Date:28-11-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability has been identified in Analytics Plus that could allow an authenticated attacker to exploit sensitive data exposure and escalate privileges within the system.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2024-52323) has been identified in Analytics Plus that could allow an authenticated attacker to exploit sensitive data exposure and escalate privileges within the system.

Vulnerabilities Details:

- **CVE-2024-52323**
- **Severity:** High
- **Impact:** This vulnerability enables an attacker to perform admin actions, such as adding or removing users and altering configurations.

Impacted Versions:

- All Analytics Plus builds below 6100

Fixed Version:

- Analytics Plus Build 6100 (Released on November 27, 2024)

RECOMMENDATIONS:

Organizations using Analytics Plus should upgrade to fixed version immediately to mitigate the risk posed by this 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/analytics-plus/CVE-2024-52323.html>