مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Packet Power Devices

Tracking #:432317594

Date:12-08-2025

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 INTELLGIENCE 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 critical authentication bypass vulnerability in Packet Power's EMX and EG products, which allows attackers to gain full access to affected devices without credentials.

TECHNICAL DETAILS:

The Packet Power Monitoring and Control Web Interface fails to enforce authentication mechanisms by default. This allows any attacker with network access to view and manipulate operational data, alter device configurations, and potentially disrupt or control connected systems, all without needing valid credentials.

The vulnerability is especially concerning in environments where these devices are used for **data center power monitoring** and **industrial control**, making them critical to infrastructure safety.

Vulnerability Details:

- **Vulnerability ID**: CVE-2025-8284
- **Severity**: Critical
- **CVSS v3 Score**: 9.8
- **Component Affected**: Packet Power Monitoring and Control Web Interface
- **Vulnerability Type**: Missing Authentication / Unauthorized Access

Affected Versions:

- EMX: Versions prior to 4.1.0
- EG: Versions prior to 4.1.0

Fixed Version:

- EMX & EG: Version 4.1.0

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed updates 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.cisa.gov/news-events/ics-advisories/icsa-25-219-05