مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Authentication Bypass Vulnerability in FreePBX

Tracking #:432319001

Date:20-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical security vulnerability has been identified in FreePBX that could allow unauthenticated attackers to gain unauthorized access to User Control Panel (UCP) portals through hard-coded credentials left unchanged after deployment.

TECHNICAL DETAILS:

A critical security vulnerability has been identified in FreePBX that could allow unauthenticated attackers to gain unauthorized access to User Control Panel (UCP) portals through hard-coded credentials left unchanged after deployment.

Vulnerability Details

- CVE ID: CVE-2026-46376
- CVSS Score: 9.1 (Critical)
- CWE: CWE-798 – Use of Hard-coded Credentials
- Attack Vector: Network
- Authentication Required: No
- User Interaction: None

Affected Versions

- Userman module in FreePBX 16 before version 16.0.45
- Userman module in FreePBX 17 before version 17.0.7

Patched versions

- Userman (FreePBX 16) 16.0.45
- Userman (FreePBX 16) 17.0.7

RECOMMENDATIONS:

- Organizations using internet-facing FreePBX systems are strongly advised to patch affected versions immediately and review configurations for default or weak credentials.

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://github.com/FreePBX/security-reporting/security/advisories/GHSA-m55x-h47x-v3gx