مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Authentication Bypass Vulnerability in Yubico's PAM Package

Tracking #:432316758

Date:17-01-2025



TLP: WHITE

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Yubico has disclosed an authentication bypass vulnerability in its pam-u2f package, which affects macOS and Linux systems using YubiKeys or other FIDO-compliant authenticators for authentication.

## TECHNICAL DETAILS:

Yubico has disclosed an authentication bypass vulnerability (CVE-2025-23013) in its pam-u2f package, which affects macOS and Linux systems using YubiKeys or other FIDO-compliant authenticators for authentication.

**Vulnerability Overview:**
CVE-2025-23013 is an authentication bypass vulnerability in Yubico's pam-u2f package. The issue stems from the pam_sm_authenticate() function's ability to return a PAM_IGNORE response under certain error conditions, such as memory allocation failures or missing configuration files. This response can lead to improper authentication decisions, potentially allowing attackers to bypass primary or secondary authentication factors.

**Affected Systems:**

- macOS and Linux systems using pam-u2f versions prior to 1.3.1
- Systems utilizing YubiKeys or other FIDO-compliant authenticators for authentication

**Fixed Version:**

- pam-u2f version 1.3.1 or later

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://developers.yubico.com/pam-u2f/Releases/