مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Persistence Vulnerability in PyPI

Tracking #:432317078

Date:15-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the Python Package Index (PyPI) team addressed a security flaw affecting its Organizations feature.

TECHNICAL DETAILS:

On April 14, 2025, the Python Package Index (PyPI) team addressed a security flaw affecting its Organizations feature. The issue allowed user privileges to persist after removal from an organization, posing a potential unauthorized access risk to sensitive package management operations.

Technical Details

- **Vulnerability Type:** Privilege Persistence / Improper Access Control
- **Discovery Date:** April 14, 2025
- **Issue Description:**
  When a user was removed from a PyPI Organization, certain team-level permissions were not fully revoked, potentially enabling continued access to sensitive actions like package uploads, deletions, or membership changes.
- **Root Cause:**
  The issue originated from logic in the **initial development of the Organizations feature**, introduced on **April 20, 2023**. During removal operations, residual privilege artifacts were not correctly cleaned up.
- **Exposure:**
  - Only **two real instances** were identified
  - **No evidence** of exploitation or unauthorized use
  - Impacted users were individually notified
- **Mitigation Actions Taken:**
  - Hotfix implemented and deployed
  - Public pull request opened for transparency
  - Full audit of all Organizations
  - Validation that no further issues persisted

RECOMMENDATIONS:

- **Review and Audit Privilege Management:** Organizations using PyPI or similar platforms should regularly audit user and team privileges, especially after user removal or role changes.
- **Implement Automated Privilege Revocation:** Ensure that privilege revocation is immediate and comprehensive upon user removal from any organizational structure.
- **Monitor for Unusual Access Patterns:** Employ monitoring solutions to detect and alert on anomalous access or privilege escalation events.
- **Stay Informed on Platform Security Updates:** Subscribe to security advisories from PyPI and other critical platforms to receive timely notifications of vulnerabilities and patches

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://blog.pypi.org/posts/2025-04-14-incident-report-organization-team-privileges/