مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Privilege Escalation Vulnerability in YubiKey Manager GUI

Tracking #:432315780

Date:23-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a security vulnerability in YubiKey Manager GUI that could allow for privilege escalation on Windows systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE: CVE-2024-31498**
- **CVSS 3.1: 7.7**
- Yubico has identified a security issue in YubiKey Manager GUI (ykman-gui) that could lead to unexpected privilege escalation on Windows. This vulnerability affects versions of the software prior to 1.2.6 and impacts installations on Windows due to the requirement for Administrative permissions to interact with FIDO authenticators. The issue arises because if a user runs the YubiKey Manager GUI as Administrator, browser windows opened by the GUI may also be opened as Administrator, which could be exploited by a local attacker to perform actions as Administrator.

Affected Software's:

- Versions prior to 1.2.6. The issue impacts installations on Windows because Windows requires Administrative permissions to interact with FIDO authenticators. For other operating systems, YubiKey Manager GUI should not be run with elevated permissions.

Fixed Versions:

- YubiKey Manager GUI 1.2.6

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by YubiKey.

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.yubico.com/support/security-advisories/ysa-2024-01/