مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

LPE vulnerability in iTunes

Tracking #:432316365

Date:07-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a local privilege escalation vulnerability in iTunes, allowing attackers to gain SYSTEM-level access on Windows machines.

TECHNICAL DETAILS:

A local privilege escalation (LPE) vulnerability, identified as CVE-2024-44193, has been discovered in iTunes version 12.13.2.3, allowing attackers to gain SYSTEM-level access on Windows machines. This vulnerability stems from improper handling of user permissions within the directory **C:\ProgramData\Apple***, enabling low-privileged users to exploit the AppleMobileDeviceService.exe component. Security researcher has published the technical details and proof-of-concept for this vulnerability.

Vulnerability Details:

- CVE Identifier: CVE-2024-44193
- CVSS Score: 8.4 (High)
- Affected Software: iTunes for Windows versions prior to 12.13.3
- Attack Vector: Local
- Privileges Required: None (local access sufficient)
- User Interaction: Required (restart of the service)

Fixed Version:

- iTunes 12.13.3

RECOMMENDATIONS:

- Immediate Update: Users must upgrade to iTunes version 12.13.3 or higher to mitigate this vulnerability.
- Review User Permissions: Organizations should audit user permissions on sensitive directories, particularly those that run services with elevated privileges.

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://support.apple.com/en-us/121328