مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in iTerm2

Tracking #:432316705

Date:06-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in iTerm2, a popular terminal emulator for macOS, which could be exploited to gain unauthorized access to sensitive data on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2025-22275
- CVSS score 9.3 Critical
- A critical security vulnerability exists in iTerm2. This flaw could lead to unauthorized access to sensitive user data.
- The vulnerability stems from a bug in the SSH integration feature, which inadvertently logs user input and output to a file (/tmp/framer.txt) on the remote host. This file is potentially readable by other users on the same host, exposing sensitive information such as passwords, private keys, and confidential data transmitted during SSH sessions.

Affected Versions:

- iTerm2 versions 3.5.6, 3.5.7, 3.5.8, 3.5.9, and 3.5.10
- Beta versions 3.5.6 and later

Users are at risk if they meet the following criteria:

1. Used iTerm2 versions 3.5.6 through 3.5.10
2. Utilized the SSH integration feature
3. Connected to remote hosts with Python 3.7 or later installed in its default search path.

This includes users who used the it2ssh command or configured their iTerm2 profiles to use SSH integration with the "SSH" command option.

Mitigations:

- Install iTerm2 version 3.5.11or later
- **Delete compromised files**: Remove the /tmp/framer.txt file from any potentially affected remote hosts.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by iTerm2.

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://nvd.nist.gov/vuln/detail/CVE-2025-22275