



مجلس الأمن السيبراني

CYBER SECURITY COUNCIL



Firmware Updates-Apple Products

Tracking #:432315991

Date:27-06-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Apple has addressed a security vulnerability in AirPods and Beats firmware that could have allowed an attacker in close proximity to gain unauthorized access to victim headphones.

TECHNICAL DETAILS:

Apple has addressed a security vulnerability in AirPods and Beats firmware that could have allowed an attacker in close proximity to gain unauthorized access to victim headphones. This vulnerability (**CVE-2024-27867**) relates to an authentication issue during the connection process.

- Affected Products: AirPods (2nd generation and later), AirPods Pro (all models), AirPods Max, Powerbeats Pro, and Beats Fit Pro
- Vulnerability: CVE-2024-27867 (authentication issue during connection)
- Exploitation: An attacker within Bluetooth range could potentially spoof a connection request and gain access to your headphones.
- Impact: Unauthorized access to your headphones could allow an attacker to eavesdrop on your conversations.
- Patched Firmware Versions: AirPods Firmware Update 6A326, AirPods Firmware Update 6F8, Beats Firmware Update 6F8

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the firmware as soon as possible.

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/HT214111>