13 popular applications have serious security vulnerabilities, users need to update immediately

Apple and The Citizen Lab have just discovered a serious security vulnerability, affecting a series of popular applications and millions of Internet users.

Picture 1 of 13 popular applications have serious security vulnerabilities, users need to update immediately

The discovered security vulnerability codenamed CVE-2023-4863 is related to heap buffer overflow in WebP due to programs and applications not managing memory well and allowing important system data to be overwritten.

If hackers successfully exploit the vulnerability, they can remotely take control of the system and launch larger-scale attacks.

This is a huge vulnerability because practically every software program or application that uses libwebp to display WebP images has problems.

The vulnerability affects a series of popular applications and OTT software such as Google Chrome, Mozilla Firefox, Microsoft Edge, Affinity, Gimp, Inkscape, LibreOffice, Thunderbird, ffmpeg, Honeyview, Telegram, Signal and 1Password.

In addition, the existence of WebP vulnerabilities also exists in many Android applications as well as cross-platform applications built with Flutter.

Google has confirmed the existence of the WebP vulnerability and has urgently released the Google Chrome 116 update to patch it.

Experts recommend that users who are using any of the applications mentioned in this article should update the software to the latest version immediately to keep their devices safer.

Apple's Security Architecture and Engineering (SEAR) team discovered and reported the WebP vulnerability in collaboration with The Citizen Lab on September 6, 2023.