Google warns of 5 serious security holes in Chrome, recommends users to update the patch immediately

Google has warned about five serious security vulnerabilities found in the Chrome browser in a recent post on the company blog.

Specifically, the identifiers of these 5 errors are CVE-2021-3798x (where x is the ordinal numbers from 1 to 5). These 5 new vulnerabilities have extremely high severity, which could put 2.6 billion users at risk. This includes the "use after free" vulnerability and the buffer overflow vulnerability.

The "use after free" vulnerability stems from a weakness in WebGL (a web graphics library) - a JavaScript API for rendering interactive 2D and 3D graphics in the browser. If successfully exploited this vulnerability, hackers can break the structure and modify the data in Chrome's executable memory. The hacker can then take over and perform remote code execution attacks on the affected victim's computer or software.

These 5 critical security vulnerabilities were discovered through the Security Rewards program (GPSRP) or simply called "bug hunt" by independent researchers.

After receiving reports of vulnerabilities, Google has developed and released patches for these 5 dangerous security flaws through Chrome update 95.0.4638.54.

Google also recommends that users update to this latest version of Chrome soon to patch these serious security holes.

If you haven't updated your Google Chrome browser to the latest version, do so now to avoid possible dangers caused by the above vulnerabilities.

many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.