Firefox releases urgent update to patch zero-day vulnerability being exploited by hackers

Mozilla has just released urgent updates for Firefox 97.0.2, Firefox ESR 91.6.1, Firefox for Android 97.3.0 and Focus 97.3.0 to fix two critical zero-day vulnerabilities being exploited by hackers.

Both are "Use-after-free (UAF)" vulnerabilities, which refer to the moment an application tries to use memory that has previously been cleaned up. When exploiting this type of vulnerability, the hacker will make the program cashed at the right time to allow the execution of commands on the device without privileges.

The UAF vulnerability is considered serious because it allows hackers to execute nearly any command remotely, including downloading malicious code to access and exploit deeper into the device.

Two zero-day vulnerabilities have just been patched by Mozilla with tracking codes CVE-2022-26485 and CVE-2022-26486 related to XSLT and WebGPU IPC Framework parameter processes respectively. According to Mozilla, hackers are actively exploiting these two vulnerabilities, so users should quickly update Firefox.

Chinese security experts from Qihoo 360 ATA company discovered and reported these vulnerabilities to Mozilla. Although Mozilla has not announced the method of exploiting the vulnerability, it is likely that hackers will trick users into accessing fake websites containing malicious code.

Due to the dangerous nature of the vulnerabilities and they are still being actively exploited, Mozilla recommends that all Firefox users update their browsers immediately.

You can check for updates manually by going to Firefox menu > Help > About Firefox. Firefox will then automatically check for, download and install the latest update, and then notify you to restart the browser to complete the update process.