Vulnerability in WinRAR puts users at risk of being attacked

A security researcher from the Zero Day Initiative (ZDI) recently announced a critical security flaw in WinRAR, leaving users' systems vulnerable to attack.

This vulnerability, codenamed CVE-2023-40477, was discovered in June. Currently, the developer RARLAB has released a patch.

Picture 1 of Vulnerability in WinRAR puts users at risk of being attacked

WinRAR is a file compression and decompression application popular with Windows computer users. This vulnerability appears in the processing of the "recovery volume", a step in the decompression process of this software. An attacker could trick a user into opening a specially crafted compressed file with the hacker's intent, then take advantage of a newly discovered vulnerability in WinRAR to execute arbitrary code on the victim's system.

According to experts, this is not a very serious vulnerability with a score of 7.8 because the exploitation depends on the user's actions.

However, according to Bleeping Computer, for hackers, tricking users into opening the file is not too much of a challenge. The number of WinRAR users is very large around the world, so the possibility of successful exploitation by hackers is also quite high.

Developer RARLAB has released patch 6.23 to fix this problem and also fix another critical error in file initialization that causes some special archives to have problems compressing. Users should update soon to ensure safety.

Microsoft is said to be testing a feature that allows users to compress files, supporting current popular compression formats such as RAR, 7-Zip and GZ built into Windows 11. If this feature officially added, WinRAR as well as third-party software will be used less often.